(U) Counterterrorism Policy Directive and Policy Guide

(U) Federal Bureau of Investigation

(U) Counterterrorism Division

(U) 0775DPG

(U) Published Date: April 1, 2015

(U) Review Date: April 1, 2018

Derived from: FBI NSICG 20130301
Classified by: F48M57K72, FBI/CTD/PCU
Declassify on: 20400205

(U) Note: This document incorporates the Policy Directive and the Policy Guide.

FEDERAL BUREAU OF INVESTIGATION
POLICY DIRECTIVE

0775PG

1. Policy Directive Title.	*Counterterrorism Policy Guide*
2. Publication Date.	2015-04-01
3. Effective Date.	2015-04-01
4. Review Date.	2018-04-01

5. Primary Strategic Objective.
A1-Protect US from terrorist and foreign intelligence activity.

6. Authorities:

Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), dated December 1, 2008.

7. Purpose:

The purpose of this policy is to promulgate the *Counterterrorism Policy Guide* (CTPG).

8. Policy Statement:

8.1. All Federal Bureau of Investigation (FBI) employees, detailees, contractors, task force members, and others responsible for performing counterterrorism operations in furtherance of the mission of the FBI must comply with the policies and procedures contained in the CTPG, which are consistent with the laws, rules, and regulations governing FBI investigations, operations, programs, and activities. See the CTPG for these policies and procedures.

8.2. Any revisions, amendments, or updates to this PG must be coordinated through the Internal Policy Office (IPO) and the Counterterrorism Division (CTD) division policy officer (DPO) and other relevant stakeholders (as determined by IPO and the proponent division). Resulting changes must then be approved by the CTD assistant director (AD) and the National Security Branch executive assistant director (EAD), as appropriate.

9. Scope:

This directive and the policies and procedures contained in the CTPG apply to all FBI employees, detailees, contractors, task force members, and others responsible for performing counterterrorism operations.

10. Proponent:

Counterterrorism Division

11. Roles and Responsibilities:

See the CTPG.

12. Exemptions:

None

13. Supersession:

This PG supersedes Policy Directive (PD) 0494D, *Counterterrorism Policy Guide*, and the *Counterterrorism Policy Guide*, 0494PG.

14. References, Links and Forms:

14.1. References

14.1.1. FBI *Domestic Investigations and Operations Guide* (DIOG) dated October 16, 2013, and any approved, subsequent iterations.

14.1.2. For additional references, key words, and links, please see the CTPG.

14.2. Acronyms

14.2.1. AD: assistant director

14.2.2. AGG-Dom: *Attorney General's Guidelines for Domestic FBI Operations*

14.2.3. CTD: Counterterrorism Division

14.2.4. CTPG: *Counterterrorism Policy Guide*

14.2.5. DPO: division policy officer

14.2.6. EAD: executive assistant director

14.2.7. FBI: Federal Bureau of Investigation

14.2.8. IPO: Internal Policy Office

14.2.9. PG: policy guide

15. Key Words, Definitions and Acronyms:

See the CTPG.

16. Appendices and Attachments:

See the CTPG.

Sponsoring Executive Approval	
Name:	Michael B. Steinbach
Title:	Assistant Director, Counterterrorism Division
Final Approval	
Name:	John Giacalone
Title:	Executive Assistant Director, Counterterrorism Division

UNCLASSIFIED

(U) Counterterrorism Policy Guide



(U) Federal Bureau of Investigation

(U) Counterterrorism Division

(U) 0775PG

(U) April 1, 2015

Derived from: FBI NSICG 20130301
Classified by: F48M57K72, FBI/CTD/PCU
Declassify on: 20400205

(U) Revised: 11/18/2015

(U) General Information

(U) Questions or comments pertaining to this policy guide can be directed to:

(U//FOUO) Federal Bureau of Investigation Headquarters/Counterterrorism Division, Division 13

(U) Office of the Assistant Director

(U//FOUO) Division point of contact: Unit chief, Policy and Compliance Unit, accessible via Outlook e-mail at [redacted]

(U) Supersession Information

(U//FOUO) This policy guide supersedes the *Counterterrorism Policy Guide* policy directive (0494D) and the *Counterterrorism Policy Guide* (0494PG).

(U) This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit or individual(s) listed in the contact section of this policy guide.

4.3. (U) Counterterrorism Program Baseline Collection Plan

4.3.1. (U) Intelligence Collection and Reporting Strategy

(U//FOUO) In an effort to standardize information and intelligence collection, as well as provide investigative guidance for both DT and IT investigations, CTD has established an investigative framework collectively referred to as "baseline collection." The purpose of baseline collection is to guide investigators in obtaining intelligence and using investigative methods during the course of each DT or IT investigation. Baseline collection is not mandatory and is not an all-inclusive listing, but rather a best practice list of items that may be accomplished when legally permissible, relevant, and consistent with the DIOG during an assessment or predicated investigation.

(U//FOUO) Baseline collection was established to provide programmatic standards in terms of the quality and thoroughness of assessments and predicated investigations. Baseline collection can help prevent gaps in investigative efforts. FOs are reminded that all investigative efforts are subject to the AGG-Dom and the DIOG. The least intrusive means of investigation/collection must be utilized under the AGG-Dom or DIOG (refer to the section on least intrusive methods in the DIOG). Baseline collection is intended to serve as a guide through the various investigative stages. Common sense will be applied when determining whether a particular item contained in the baseline collection pertains to a specific assessment or investigation. If there is doubt as to whether the appropriate authority exists in an individual investigation to address a baseline collection item, employees are to consult the chief division counsel (CDC), OGC, and/or the CTD program manager.

(U//FOUO) Supervisors may address baseline collection with case agents during investigative file reviews, and such reviews will inform many of the intelligence and collection matters required for review, in accordance with DIOG subsection 3.4.4.6. In addition to standardizing

information and intelligence collection, baseline collection will help to establish a foundation of intelligence upon which the FBI may base the decision to continue or close an assessment or investigation.

(U//FOUO) Baseline collection items are in no particular order. Furthermore, information not called for by baseline collection may also be collected if legally permissible, practical, and relevant to the investigation. Baseline collection also involves consideration of the credibility of the original information or source of information, in terms of predication. If the credibility of the original information or source is ever substantially questioned, any further investigation based upon the information or source must be reevaluated to determine whether predication continues to exist. No investigative method will be used if information is developed that significantly undermines the purpose or predication of the assessment or investigation.

(U//FOUO) This standardized approach to all CT investigations will allow CTD and FOs to more effectively and efficiently manage CT investigations. CTD will maintain an open dialogue with all FO CT supervisors in order to identify intelligence gaps, provide guidance and recommendations, and ensure all available CTD resources are appropriately utilized in each investigation.

4.3.2. (U) Assessments

(U//FOUO) In CT Type 1 & 2 assessments, investigators may, when relevant to the purpose of the assessment, collect the information that is necessary to answer the questions detailed below in Category A (refer to subsection 5.3 of this PG for a list of authorized methods). The assessment may continue until factual information is developed that warrants opening a predicated investigation or until a judgment can be made that the target does not pose a terrorism or criminal threat. Assessments may not remain open solely to collect more information if the purpose of the assessment has been achieved or if the information is not necessary to achieve the purpose. See DIOG Section 5 for additional information regarding assessments.

(U//FOUO) In CT Type 1 & 2 assessments, there are also specific, mandatory baseline collection requirements. Refer to Policy Directive (PD) 0649D, *Mandatory Baseline Collection During Counterterrorism (CT) Assessments*, for a discussion and list of these requirements.

4.3.2.1. (U) Category A Questions

(U//FOUO) To answer the Category A questions accurately, database checks will be necessary. This information is to be collected, if it can be done, with the methods authorized during an assessment.

> (U) **Note:** National security letters (NSL) and administrative subpoenas are not authorized during an assessment. Grand jury subpoenas (GJS) are limited to subscriber information only for Type 1 & 2 assessments. See DIOG section 18.5.9, "Investigative Method: Grand Jury Subpoenas – providers of electronic communication services or remote computing services for subscriber or customer information."

(U//FOUO) Category A questions are:

1. (U//FOUO) The subject's full, legal name, and aliases, if any.

(U) **Note**: Some nationalities and cultures do not distinguish between first, middle, and last names in the same manner as the United States. Thoroughness may require database checks of each of the known names put in the position of the last name.

2. (U//FOUO) The subject's date and country of birth.
3. (U//FOUO) A determination of the subject's United States person (USPER) status. Refer to Appendix G [SECRET//NOFORN document] of the DIOG.
4. (U//FOUO) The subject's passport number(s) and country of issuance.
5. (U//FOUO) The subject's social security number (SSN) (if the subject is an USPER) and any other unique identifying numbers relevant to database checks (e.g., alien registration number and driver's license number).
6. (U//FOUO) The subject's telephone number(s), e-mail address(es), and/or other Internet communication media utilized by the subject.
7. (U//FOUO) The subject's current address and any prior address(es), particularly if it appears that the subject recently relocated. It will normally be unnecessary to ascertain previous addresses more than five years old.
8. (U//FOUO) The subject's current place of employment and position.

(U//FOUO) When available identifying information has been obtained, it may be used to conduct the checks necessary to answer the following questions. These questions are generally relevant to all CT assessments. Only information about the subject that is relevant to answering these questions or otherwise resolving the assessment may be documented in FBI files. Employees are to avoid collecting or documenting personal information about the subject that is not relevant to the assessment. The questions below are not in any particular order and are not all-inclusive. The least intrusive means, if reasonable, based upon the circumstances of the investigation is to be considered to answer each question. While some databases are suggested, open source information may also be checked to answer these questions.

9. (U//FOUO) Has the subject ever been the target of, or been referenced in, another FBI investigation? Query the FBI's central recordkeeping system, Guardian and/or the Investigative Data Warehouse (IDW), or other FBI recordkeeping systems.
10. (U//FOUO) Has the subject's current address or place of work been referenced in other FBI investigations? Query the FBI's central recordkeeping system, IDW, or other FBI recordkeeping systems.
11. (U//FOUO) Does the subject have a criminal history (a conviction or an arrest) that is relevant to the assessment's purpose? Profit-driven crimes such as fraud, identity theft, and dealing illicit narcotics may be as relevant to a CT assessment as crimes of violence and/or firearms violations. Any active arrest warrant must be noted in the assessment. Query federal, state, and local criminal/law enforcement systems, such as the National Crime Information Center (NCIC), state Department of Motor Vehicles (DMV), and other local systems.

12. (U//FOUO) Is there reason to believe that the subject has been in telephone contact with subjects of other FBI investigations? If so, compare the relevant data concerning the subject's telephone number with FBI databases, and, as appropriate, conduct link/timeline analysis. Query Telephone Application (TA), IDW, Polaris/Clearwater, Data Warehouse System (DWS), and Data Loading and Analysis System (DaLAS).

13. (U//FOUO) Is there reason to believe that the subject has been in e-mail contact with subjects of other FBI investigations? If so, compare relevant data concerning the subject's e-mail account(s) with FBI databases, and, as appropriate, conduct link/timeline analysis. Query IDW, Polaris, Clearwater, DWS, and DaLAS.

14. (U//FOUO) Is there any reason to believe that the subject has access to hazardous or explosive materials? An indication of such may include any special licenses or permits (e.g., a commercial driver's license [CDL] with a hazardous materials [Hazmat] endorsement) that authorize the subject to obtain or possess explosives or other dangerous materials.

15. (U//FOUO) Is there any reason to believe that the subject has purchased or is licensed to possess firearms or other weapons? If so, run NCIC checks and/or contact local Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) representatives or any available state database in the relevant jurisdiction to collect responsive records and information.

16. (U//FOUO) Is there any reason to believe, considering the subject's background, employment history, and criminal history, that the subject has received specialized training or experience or has knowledge that is relevant to the investigation (e.g., military service, law enforcement, firearms, explosives, pilot/aviation, scuba diving, engineering, architectural, computer science, pharmaceutical, chemical, biological, radiological, nuclear, or similar subjects)?

17. (U//FOUO) Within the past year, has the subject traveled abroad to a country(ies) relevant to the assessment? Query the TECS, Airline Reporting Corporation (ARC), DOS's Consular Consolidated Database (CCD), and/or a DOS liaison requesting an USPER subject's passport application history.

18. (U//FOUO) Does the subject live alone or with another adult(s)? If the subject lives with another adult(s), is there any reason to believe said adult(s) is involved with the matter under assessment?

19. (U//FOUO) For a subject with an international nexus, does the USIC have any relevant information about the subject? Query the FBI's central recordkeeping system, Guardian, IDW, the National Counterterrorism Center (NCTC) Online, a DOS liaison (non-USPERs only), and/or other USIC databases.

 (U//FOUO) **Note**: The appropriate CTD program management unit can assist in seeking information from foreign intelligence/law enforcement agencies. Contacting foreign agencies is a relatively intrusive step because it reveals the FBI's interest in the subject, especially if that subject may travel to that foreign country in the future. Accordingly,

such contacts must be coordinated through CTD and only when the available information justifies this level of intrusion.

20. (U//FOUO) Could the subject's job or other activities reasonably support the covert collection or transfer of money or funds for terrorism or criminal purposes (e.g., export/import, overseas shipping, cash business)? If so, does the subject have any previously identified suspicious monetary transactions? Review suspicious activity Reports (SAR), Currency Transaction Reports (CTR), and Currency or Monetary Instrument Reports (CMIR). Query the Financial Crimes Enforcement Network's (FinCEN) Gateway database.

4.5. (U) Counterterrorism Disruptions

(U//FOUO) The disruption of a predicated CT investigation occurs when a deliberate law enforcement or intelligence action alters or impedes the normal and effective operations of an individual, a group, an organization, or an enterprise engaged in terrorism or activities in preparation for, or support thereof. CT disruptions may only be claimed in DT or IT investigations and foreign police cooperation matters related to DT or IT.

4.5.1. (U) Disruption Strategy

(U//FOUO) The long-term goal of a DT or an IT investigation is to develop intelligence regarding all aspects of the terrorist threat. Properly targeted responses will gather all available intelligence prior to conducting overt disruption activities, while maintaining the interests of public safety. The value of the intelligence collection in relation to the nature and significance of the threat and the negative impact of allowing the subject's activities to continue must be considered when making the decision on when and whether to disrupt a subject(s).

(U//FOUO) If the risk to public safety is too great or if all significant intelligence has been collected and/or the threat is otherwise resolved, investigators may, with program management unit coordination and concurrence, implement a disruption strategy.

4.5.2. (U) Definition of a Counterterrorism Disruption

(U//FOUO) A CT disruption is an affirmative action(s) by the FBI or a federal, state, local, or foreign partner in coordination with the FBI, which neutralizes the threat posed by an FBI terrorism subject (i.e., an individual, a group, an organization, or an enterprise). Only one office

may claim the disruption of a given subject as a statistical accomplishment. Any other office that makes a significant contribution to the disruption (e.g., serves a warrant or conducts interviews) may claim a disruption assistance as a statistical accomplishment. In the event FOs disagree as to which office will claim the disruption, the issue must be referred to the appropriate CTD program management section for resolution and decision.

(U//FOUO) A successful disruption strategy may employ a range of tools to possibly include arrests, deportations, interviews, or source-directed operations to effectively disrupt a subject's activities. As a best practice, when warranted, all subject interviews will specifically address the subject's activities and potential recruitment as a CHS. Examples of some investigative actions, short of a criminal charge, that could disrupt a terrorist subject include:

- (U//FOUO) A targeted interview of the subject(s).
- (U//FOUO) Source-directed activities (e.g., providing disinformation).
- (U//FOUO) A media campaign to publicize activities, in accordance with Office of Public Affairs (OPA) policies.
- (U//FOUO) Revoking an immigration visa.
- (U//FOUO) The seizure of financial assets.

4.5.3. (U) Disruption Reporting

Superseded by PD 0523D, *Guidance for Claiming Investigative and Intelligence Statistical Accomplishments*, dated 6/30/2012.

5. (U) Counterterrorism Assessments

5.1. (U) Purpose of Counterterrorism Assessments

(U//FOUO) For the policies and rules regarding the conduct of assessments,[1] refer to DIOG Section 5.

(U//FOUO) A Guardian entry must be completed on all counterterrorism incidents, such as a threat report or SAR, even when a predicated investigation is opened. In those instances where a predicated matter (PI, full investigation, or EI) is opened, a minimum amount of general information regarding the matter must be entered into Guardian, and then the Guardian lead may be closed for the purposes of opening the PI/full investigation.

5.2. (U) Types of, and Basic Rules for, CT Assessments

(U//FOUO) FOs and CTD will utilize one of two models when conducting CT assessments:

1. (U//FOUO) Guardian-based (Type 1 & 2 assessments)
2. (U//FOUO) Assessment investigative file-based (Type 3 and Type 4 assessments)

5.2.1. (U//FOUO) Guardian-Based (Type 1 & 2 Assessments)

(U//FOUO) Although Guardian is not an investigative file management system, it does track and manage threats and SARs during the information collection and lead mitigation period, as well as allow for the analysis of trends and patterns of threats and suspicious activity. FOs, Legats, and other FBI entities must enter all reports of actual or potential terrorist threats and suspected terrorist activity occurring within the United States or against U.S. interests abroad into Guardian.

(U//FOUO) Generally, items entered into Guardian are those activities, incidents, or observations (including citizen complaints) that may have a nexus to terrorism and may be utilized to detect, obtain information about, or prevent and protect against federal crimes or threats to the national security.

(U//FOUO) An FO must create a Guardian record to summarize the nature of all terrorism-related threats and/or SARs. If the FO opens a predicated investigation subsequent to the Guardian entry, the FO must update the Guardian record within the "Disposition" tab and include the predicated investigation file number in the closing disposition. The Guardian record must also be serialized into the FBI's central recordkeeping system investigative file for the predicated investigation. Also, if the FO sends an [redacted] to the Strategic Information and Operations Center (SIOC), CT Watch, and the appropriate program management unit regarding a terrorism-related threat, the FO must enter the event or suspicious activity into Guardian (unless it is already part of an open investigation and/or was previously entered into Guardian).

[1] (U) All uses of the word "assessment" may be presumed to mean an AGG-Dom-authorized level of investigative activity, unless indicated otherwise. For further context on meanings, refer to Appendix A.

(U//FOUO) An FO may enter information obtained from a documented CHS into Guardian, however, efforts must be undertaken to protect the CHS's confidentiality and ensure that the entry is in compliance with Guardian protocols. Any information that could identify the CHS (e.g., code name) may not be entered in Guardian. Refer to the Guardian Intranet page.

(U//FOUO) Program management and oversight responsibility for Guardian assessments has been assigned to the ART within the CT Watch. Any threat mitigation issues or potential policy violations found in a Guardian assessment by the ART must be brought to the responsible office's attention and will require a response and/or action to bring the incident into compliance. If an FO or a division fails to correct or clarify the Guardian incident within a reasonable timeframe, *ART will set an immediate action lead via EC to the responsible office. This EC will be maintained* in the appropriate investigative file and a copy provided to the ART file.

5.2.1.1. (U) Use of Zero Sub-Assessment Files

(U//FOUO) All Guardian-based assessments that are not converted to predicated investigations will be uploaded to a zero sub-assessment file upon final disposition of the Guardian lead. These zero sub-assessment files may be either FBIHQ or FO files, and one will exist for each alpha designator [redacted] FOs must maintain zero sub-assessment files as specified in the DIOG. Such files should contain all documentation of investigative activity, approvals, use of investigative methods, etc., generated during the course of an assessment.

5.2.2. (U//FOUO) Assessment Investigative File-Based (Type 3 or Type 4 Assessments)

(U//FOUO) Assessment investigative files are used when conducting assessments for threats and vulnerabilities (Type 3 assessments) and intelligence analysis and planning–domain analysis (Type 4 assessments). See DIOG Section 5 for further information regarding assessments.

(U//FOUO) **Note**: Type 4 assessments conducted by field intelligence groups (FIG) must abide by the DIOG and the [redacted]

(U//FOUO) The appropriate CT investigative classification must be used when opening a CT assessment [redacted] Investigative activity may not be documented in control files (see the DIOG). Refer to the CTD Templates Page.

5.3. (U) Authorized Methods

(S//NF) All investigative methods outlined in the DIOG as being authorized in an assessment may be used, with the exception of the operation of FBI CHSs outside the territorial jurisdiction of the United States.

5.4. (U) Baseline Collection Plan

(U//FOUO) During an assessment, an FO may consider, when it is relevant, practical, and legally permissible, conducting the items outlined in Category A, with respect to identifying information for each subject, in accordance with CTD's baseline collection plan outlined in subsection 4.3.2. of this PG.

5.5. (U) Opening a CT Type 1 & 2 Assessment

(U//FOUO) The initiation of a Type 1 & 2 assessment by an FO can be noted by CTD using Guardian. Formal notification is not required to a respective CTD program management unit. This lack of formal notification does not eliminate the need for FOs to keep CTD properly informed of threat information, in accordance with subsection 4.2. of this PG.

(U//FOUO) The opening of a file-based assessment must be documented with an appropriate EC, in accordance with the DIOG.

5.6. (U) Closing of a CT Assessment

(U//FOUO) Prior to closing a Guardian-based assessment, all reasonable effort must be made to reach a definitive conclusion as to the potential threat of a criminal violation(s) or national security threat(s) posed by the subject in question. If a clear and lasting decision can be made as to the potential threat, the Guardian incident must include in its disposition an answer of "Yes" or "No" to the question regarding nexus to terrorism. If there is insufficient information to make a definitive and lasting determination as to the potential threat, the disposition may be marked as "Inconclusive." Use of the inconclusive marking means that at the time of closing, all available resources and investigative avenues have been exhausted, and the FBI remains unable to conclusively determine whether or not the subject does, or might in the future, pose a threat.

(U//FOUO) The closing of a CT assessment investigative file must contain a clear statement concerning any identified criminal violation(s) or national security threat(s) and an affirmative finding that the file no longer serves an authorized purpose.

9.8. (U) Online Investigations

(S//REL TO USA, FVEY) The CITU program manages unique CT Internet investigations that target terrorists' use of the virtual realm where a Web site or online network of individuals is the target of the investigation or where Internet exploitation is the primary investigative method. CT subjects may use extremist Web sites or forums to engage in the spread of extremist ideology and other terrorist activity. Coordination with other CT program management units will occur, as necessary, to determine the appropriate program management responsibilities, based on the subject's Internet activities.

(S//REL TO USA, FVEY) The online targeting of an extremist Web site or online network is considered a sensitive method. Therefore, any information regarding the targeting of such Web sites, the public disclosure of which would reduce the effectiveness of the method, must be classified "SECRET//REL TO USA, FVEY," in accordance with NSICG, citation number INV-20. This applies to details of the method that have not been made public, even when use of the method in general has been officially acknowledged.

9.8.1. (U//FOUO) Types of Online Investigations

(U//FOUO) Outlined below are guidelines for when an investigation will be handled as an online investigation. Questions and consultation may be directed to CITU when a determination, based on the following guidelines, cannot be made by an FO.

9.8.1.1. (S//REL TO USA, FVEY) Extremist Forums and Chat Rooms

(S//REL TO USA, FVEY) Online investigations may be opened on suspected terrorists or terrorist groups that use Internet forums, chat rooms, bulletin boards, blogs, servers, and Web sites to encourage and recruit members among English-speaking audiences in Western nations. CITU has noted a trend that al-Qa'ida and its Sunni affiliates are attempting to reach non-Arabic-speaking Muslims who live in the Western world online, in efforts to communicate extremist jihadist propaganda in languages native to Western speakers. Web sites and forums espousing such propaganda contribute to the radicalization process and facilitate the recruitment of individuals into terrorist organizations and cells. Surveys of extremist-run forums have determined that English-language forums have led to the rise of terrorist cells entirely within the

borders of Western nations that are largely independent of offline interaction or direction from traditional terrorist leadership abroad.

9.8.1.2. (S//REL TO USA, FVEY) Forum Administrators

(S//REL TO USA, FVEY) Online investigations may be opened on administrators of Internet forums that are being used to facilitate international terrorist activity, to include propaganda. Past investigations have demonstrated the administrators of extremist forums are key facilitators within foreign terrorist organizations. The administrators are in contact with terrorist media cells and couriers, as well as the senior leadership of terrorist organizations. Forum administrators may include individuals who create chat rooms, bulletin boards, blogs, servers, and Web sites.

9.8.1.3. (S//REL TO USA, FVEY) Forum Participants

(S//REL TO USA, FVEY) An investigation may be considered an online investigation when it is primarily based on a subject's online activities and participation with extremist forums, chat rooms, bulletin boards, blogs, servers, or Web sites. Forum participants may include individuals whose primary activity includes the development of communications security practices and individuals acting as "virtual couriers" for terrorist organizations by passing online messages among members or leadership. Other individuals not meeting these criteria, but identified through the investigation of extremist forums or online networks, must be "spun off" for program management by the appropriate CTD program management unit and FO.

9.8.1.4. (U) Use of Online Methods

(S//REL TO USA, FVEY) An investigation may be considered an online investigation when it uses exploitation of the Internet as its primary method of intelligence collection or investigation. Examples of such methods include the use of online CHSs, online covert employees (OCE), or the electronic surveillance of Internet-based facilities.

9.8.1.5. (U) Joint Investigations

(S//REL TO USA, FVEY) An investigation may be considered an online investigation when opened at the request of a USIC or allied foreign partner to exploit terrorists' use of the Internet. As the majority of the world's Internet infrastructure (including Web site hosting) is based in the United States, it is anticipated CTD will pursue opportunities for FISA collection on U.S.-based servers when requested to do so, and when it is appropriately predicated by a USIC or allied foreign partner.

(S//REL TO USA, FVEY) Multiple agencies of the USIC, including the CIA and the National Security Agency (NSA), have robust efforts to exploit terrorists' use of the Internet. CTD actively engages these partners with the intent of establishing and properly leveraging these contacts to enhance FBI investigations against common targets. In order to facilitate information exchanges and leverage allied resources for the FBI in the development of joint operations, CTD develops relationships with allied foreign intelligence and law enforcement partners on matters involving terrorists' use of the Internet.

9.8.2. (U//FOUO) Unique Woods Procedures for FISA Collection

(S//REL TO USA, FVEY) In addition to the normal requirements of the [redacted] for FISA collection outlined in the DIOG and in subsection 12.5.4, of this PG, the following additional Woods Procedures must be followed when a CTTU-managed, USIC partner FISA package is being processed for submission to the FISC:

1. (S//REL TO USA, FVEY) The FBI declarant (typically a CTTU SSA) for the USIC package will generally receive the package via the community of interest (COI) or TOP SECRET (TS) e-mail.
2. (S//REL TO USA, FVEY) The declarant must review the package, noting the specific pages/information related to the FO responsible for the investigation, and send a TS e-mail to the respective FO, requesting a limited Woods form for the specific pages/information contained in the FISA package related to the FO's intelligence/information.
3. (S//REL TO USA, FVEY) The FO must review the specified pages/information, verify that the facts are accurate, and complete a limited Woods form with notations stating the page number and the specific paragraph and/or information verified. The limited Woods form must subsequently be sent to the CTTU declarant.
4. (S//REL TO USA, FVEY) The information described above must be maintained in the FISA Accuracy subfile established for the captioned investigation where the intelligence/information was derived. The information must contain a notation on which FISA package it verifies.

(U//FOUO) Upon completing the four steps above, FOs must:

- (U//FOUO) Print the e-mail requesting the limited Woods form.
- (U//FOUO) Print the specific pages/information from the FISA package.
- (U//FOUO) Attach copies of the documents used to verify the FO's information in the FISA package.
- (U//FOUO) Attach the signed, original Woods form.
- (U//FOUO) Forward the package to the CTTU, who will arrange transmission to DOJ's NSD/Office of Intelligence (OI).

9.8.3. (U//FOUO) Joint CTD/Cyber Division (CyD) Investigations

(S//REL TO USA, FVEY) Due to the potential for overlap regarding investigations targeting terrorists' use of the Internet, CTD and CyD have implemented the following procedures:

- (S//REL TO USA, FVEY) An FO cyber squad must immediately notify the FO CT squad upon opening a Computer Intrusions - International Terrorism (288J investigative classification) PI or full investigation. The CT squad SSA will identify a CT special agent (SA) to initiate an appropriate, parallel CT investigation and to serve as a CT POC. The

POC will ensure the leveraging of all national security tools to address the targets of the investigation.

- (S//REL TO USA, FVEY) If a CT squad determines cyber activity exists in a 415 investigation, the CT SSA must contact the cyber SSA. The cyber SSA will then assign a cyber agent as a POC. After collaborating, the cyber squad will determine to what degree, if any, the investigation involves cyber terrorist intrusion activity, and will open a 288J investigation, if appropriate. If there is no intrusion activity, but a need for technical assistance exists, the CT squad may request that the cyber squad open a 288L (Technical Support to CT) investigation.
- (S//REL TO USA, FVEY) All 352 investigations involving parallel CTD 415 investigations must include in the distribution: Counterterrorism, Attn: CXS/CITU; Cyber Division, Attn: CNSS. Each communication must be filed in both the 352 and 415 investigations.

9.8.4. (S//REL TO USA, FVEY) Online Undercover and HUMINT Operations

(S//REL TO USA, FVEY) The requirements set forth in subsection 9.6. of this PG regarding national security undercover operations apply to all online UCOs, including the Net Talon National Initiative (NTNI) (refer to subsection 9.8.5. of this PG).

(S//REL TO USA, FVEY) Any IT investigation utilizing the undercover method to investigate online extremists and/or extremist Web sites, including, but not limited to, forums, chat rooms, blogs, and other Internet technologies, must be considered a sensitive circumstance and will therefore be a Group I UCO. Initiation of CT online UCOs must be coordinated with CITU, CTUC, and the National Security Law Branch (NSLB). Such online UCOs must be evaluated by CITU and CTUC for inclusion into the NTNI (refer to subsection 9.8.5 of this PG).

9.8.4.1. (U) Deconfliction

(S//REL TO USA, FVEY) During an online investigation, it is imperative that the FO and CTD implement strong source deconfliction measures. Insufficient deconfliction, combined with the diffuse nature of the Internet, has previously resulted in resources being wasted by investigating or collecting on FBI online identities (i.e., undercover employees [UCE]/ OCEs/CHSs) who have already been investigated by other FBI offices, the USIC, and/or an allied foreign partner. Increased collaboration and coordination regarding online UCEs/OCEs/CHSs is necessary to reduce the problems of self-investigation and duplication and to enhance the FBI's overall efforts to counter terrorists' use of the Internet.

(S//REL TO USA, FVEY) CITU is the lead unit within CTD to deconflict all matters pertaining to online identities. The Net Talon database (refer to subsection 9.8.5. of this PG), maintained and operated by CITU, identifies deconfliction needs for the numerous online aliases and monikers of FBI UCEs, OCEs, CHSs, and extremist Web sites.

9.8.5. (U//FOUO) Net Talon National Initiative

(S//REL TO USA, FVEY) In May 2008, the NTNI was approved by the CTD. The NTNI is an online, undercover, national initiative constructed to strategically focus operations (using OCEs, UCEs, and CHSs) targeting terrorists' use of the Internet.

(U//FOUO) For further details regarding the Net Talon Program, refer to Section 17 of this PG.

10.6. (U//FOUO) Online Investigations

10.6.1. (U//FOUO) Types of Online Investigations

(U//FOUO) Outlined below are guidelines for when an investigation will be handled as an online investigation. Questions and consultation may be directed to DTOU when a determination, based on the guidelines below, cannot be made by an FO.

10.6.1.1. (U//FOUO) Extremist Forums and Chat Rooms

(U//FOUO) An investigation may be considered an online investigation when a suspected extremist or terrorist group uses Internet forums, chat rooms, bulletin boards, blogs, servers, and Web sites to encourage and recruit members, and the investigation is primarily focused on the online activities of the extremist(s). Web sites and forums espousing such propaganda may contribute to the radicalization process and facilitate the recruitment of individuals into domestic extremist organizations.

(U//FOUO) An investigation may be considered an online investigation when the matter targets the administrators of Internet forums. Past investigations have demonstrated the administrators of extremist forums are often key facilitators within domestic extremist organizations. The administrators are often in contact with senior leadership of the organizations or are members of

the organizations themselves. Forum administrators may include individuals who create chat rooms, bulletin boards, blogs, servers, and Web sites.

10.6.1.2. (U//FOUO) Forum Participants

(U//FOUO) An investigation may be considered an online investigation when the matter is primarily based on the subject's online activities and participation with extremist forums, chat rooms, bulletin boards, blogs, servers, or Web sites. Forum participants may include individuals whose primary activity includes the development of communications security practices or individuals acting as "virtual couriers" for domestic extremist organizations by passing online messages among members or leadership. Other individuals not meeting these criteria, but identified through the investigation of extremist forums or online networks, will be "spun off" for program management by the appropriate FO and DT program management unit.

10.6.1.3. (U//FOUO) Use of Online Methods

(U//FOUO) An investigation may be considered an online investigation when it uses exploitation of the Internet as its primary method of intelligence collection or investigation. Examples of such methods include the use of online sources, UCEs, or electronic surveillance of Internet-based facilities.

10.6.2. (U//FOUO) Joint CTD/CyD Investigations

(U//FOUO) Due to the potential for overlap regarding investigations targeting extremist use of the Internet, CTD and CyD have implemented the following procedures:

- (U//FOUO) Upon the opening of either a Computer Intrusions - Domestic Terrorism (288K classification) PI or full investigation, the FO cyber squad must immediately notify the FO DT squad. The DT squad SSA will identify a DT SA to initiate an appropriate parallel CT investigation and serve as a DT POC. The POC will ensure the leveraging of all national security tools to address the targets of the investigation.
- (U//FOUO) If a DT squad determines cyber activity exists in a DT investigation, the DT SSA must contact the cyber SSA. The cyber SSA will then assign a cyber agent as a POC. After collaborating, the cyber squad will determine to what degree, if any, the investigation involves cyber terrorist intrusion activity, and open a 288K investigation, if appropriate. If there is no intrusion activity, yet technical assistance needs exist, the DT squad may request that the cyber squad open a 288G (Technical Support to DT) investigation.
- (U//FOUO) All 288G and 288K investigations involving parallel DT investigations must include in the distribution: Counterterrorism, Attn: DTOU; and Cyber Division, Attn: NSCU. Each communication must dual caption the investigation ID number to include both the 288 and the appropriate DT classifications.

10.6.3. (U//FOUO) Online Undercover and HUMINT Operations

(U//FOUO) The requirements set forth in subsection 10.5. of this PG regarding DT undercover operations apply to all online DT UCOs.

10.6.3.1. (U) Deconfliction

(U//FOUO) During an online investigation, it is imperative that the FO and DTOU implement strong source deconfliction measures. Insufficient deconfliction, combined with the diffuse nature of the Internet, has previously resulted in resources being wasted by investigating or collecting on FBI UCEs/OCEs/CHSs who have already been investigated by other FBI offices, the USIC, and/or allied foreign partners. Increased collaboration and coordination regarding online UCEs/OCEs/CHSs is necessary to reduce the problems of self-investigation and duplication, and it enhances the FBI's overall efforts to counter terrorists' use of the Internet.

(U//FOUO) DTOU must utilize the Net Talon database for deconfliction of all DT online investigations. Refer to subsection 17.5. of this PG for more information on the Net Talon Database.

11. (U) Terrorist Watchlisting

11.1. (U) Watchlisting Basics

(U//FOUO) The USG maintains a consolidated list of individuals who are known or suspected of being terrorists. This list, known as the Terrorist Screening Database, is maintained by the Terrorist Screening Center (TSC). The submission of an individual to maintenance/modification of and appropriate removal of the records within the TSDB is referred to as watchlisting.

(U//FOUO) The USG's consolidated terrorist watchlist is a critical tool for screening: (1) at U.S. borders and ports of entry; (2) passport and visa applicants; (3) aircraft passengers and crew members; (4) during federal and domestic law enforcement encounters; or (5) other approved activities that have a substantial bearing on homeland security. The watchlist can quickly and accurately notify the user that he or she has encountered a known or suspected terrorist (KST), and it provides instruction on how to respond to the encounter.

(U//FOUO) TREX is responsible for ensuring all subjects of FBI terrorism investigations are appropriately nominated to, and/or removed from, the TSDB and all eligible supporting systems. TREX also ensures that records in the TSDB and supporting systems are modified, as appropriate. A nomination is accomplished through the submission of a watchlist nomination, modification, or removal to TREX (refer to subsection 11.6 of this PG).

11.1.1. (U) The Terrorist Screening Center

(U//FOUO) The TSC was established in 2003 by Homeland Security Presidential Directive 6 (HSPD-6), which directed the establishment of an organization that would consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The TSC is a multiagency entity administered by the FBI, with the mission of facilitating and assisting in the protection against terrorism by:

- (U//FOUO) Consolidating the USG's approach to terrorism screening.
- (U//FOUO) Providing for the appropriate and lawful use of terrorist identity information in screening processes.
- (U//FOUO) Maintaining consolidated, thorough, accurate, and current information on terrorist identities.
- (U//FOUO) Sharing information globally and between the federal, state, local, territorial, and tribal law enforcement and intelligence communities.
- (U//FOUO) Conducting these activities in a manner consistent with the U.S. Constitution and applicable U.S. laws protecting privacy and civil liberties.

(U//FOUO) To ensure the TSDB contains the most thorough, accurate, and current information, TSC personnel review individual TSDB records throughout the watchlisting process, including, but not limited to, at the time of nomination and/or modification, at the time of a screening encounter with a watchlisted subject, and at the time a watchlisted subject submits a redress inquiry with a screening agency.

(U//FOUO) The TSC receives "identifiers" of KSTs from the following two sources: (1) the NCTC regarding international terrorists and (2) directly from the FBI regarding domestic terrorists. Identifiers include biographical information such as date of birth (DOB), place of birth, SSN, or biometric information such as photographs or fingerprints. The identifiers of suspected terrorists in the TSDB are deemed "For Official Use Only" (FOUO) and are for watchlisting purposes only.

11.2. (U) Civil Liberties

(U//FOUO) To protect civil liberties and privacy, every watchlisting nomination must meet the watchlisting standard (refer to subsection 11.3. of this PG). The watchlisting of individuals based solely on activities protected by the First Amendment, on the race, ethnicity, national origin, or religion of the subject; or for political or retaliatory purposes is prohibited. Any proposed nomination for watchlisting that involves a SIM (refer to the DIOG section on sensitive investigative matters) will be brought to the attention of TSC, CTD, OGC, and DOJ officials, as appropriate. FBI personnel must strive to ensure that the data submitted is accurate, thorough, and current. Also, personnel must ensure watchlist records are updated on a timely basis to limit any potential adverse consequences to watchlisted individuals and to reduce the potential for misidentification.

11.2.1. (U) USPER Status

(U//FOUO) A subject's USPER status does not prevent the subject's nomination for entry into the TSDB. In accordance with the TSC's *Watchlisting Guidance, March 2013*, § 3.15, nominations of USPERs must be made based on information of known reliability or where there exists additional corroboration or context supporting reasonable suspicion. To meet these requirements, all FBI nominations are reviewed by TREX and TSC, which confirm that the watchlisting standard has been met. While TSDB includes USPER subjects, USPER status may affect a subject's export to a particular supported system.

11.3. (U) Watchlisting Standard

(U//FOUO) In order to nominate a subject for entry into the TSDB and all eligible supported systems, the FBI must have a reasonable suspicion to believe that the subject is a KST or an authorized exception. To meet this standard, the FBI must have "articulable" intelligence or information which, based on the totality of the facts, and taken together with rational inferences from those facts, reasonably warrants a determination that the subject is known or is suspected to be (or has been) knowingly engaged in conduct constituting, in preparation for, in aid of, or related to, terrorism or terrorist activities. There must be an objective, factual basis for the nominator to believe that the individual is a KST. Mere guesses or "hunches" are not enough to constitute a reasonable suspicion that an individual is a KST. For additional detailed information on the watchlisting standard, refer to the TSC's *Watchlisting Guidance, March 2013*, or its successor.

(U//FOUO) The DIOG authorizes the initiation of a PI based on any "allegation or information" indicative of criminal activity or threats to national security. In order for PI subjects to be watchlisted, the allegation or information used to predicate the investigation must also meet the reasonable suspicion standard for watchlisting. The DIOG authorizes the initiation of a full

investigation based on an "articulable factual basis" of possible criminal and national threat activity. The articulable, factual basis used to open a terrorism full investigation does meet the reasonable suspicion standard for watchlisting.

(U//FOUO) Subjects of Guardian assessments are not to be submitted to TREX for watchlisting, nor may terrorist group or organization names be nominated for entry into the TSDB. Nominations may not be based on source reporting deemed unreliable. Suspicious activity alone that does not rise to the level of a reasonable suspicion, or an authorized exception, is not a sufficient basis to watchlist an individual. The objective, factual basis linking a specific individual to terrorism or terrorist activities is also known as particularized derogatory information, which is the basis for adding the subject of an FBI investigation to the TSDB.

(U//FOUO) In making a reasonable suspicion determination, the FBI may consider behavioral indicators known to be associated with particular known or suspected terrorists in the past. The need to protect civil liberties, however, requires that such indicators not be judged in isolation. Each indicator must be viewed in the context in which it occurs and considered in combination with all other known information to ensure that any nomination based in whole or in part on this behavior comports with the standards set forth above. Examples of some existing behavioral indicators include:

- (U//FOUO) Attendance at training camps known to the USIC as facilitating terrorist activities.
- (U//FOUO) Attendance at schools/institutions identified by the USIC as teaching extremist ideology, including the justification of the unlawful use of violence or violent extremism.
- (U//FOUO) Repeated contact with individuals identified by the USIC as teaching or espousing ideology that includes the justification of the unlawful use of violence or violent extremism.
- (U//FOUO) Travel for no known lawful or legitimate purpose to a locus of terrorist activity.

(U//FOUO) Additional guidance and specific investigation examples for the reasonable suspicion standard can be found on the TREX Intranet site and on the TSC Intranet site.

11.3.1. (U) Exceptions

(U//FOUO) The National Security Council has approved several instances in which an individual who does not meet the reasonable suspicion standard may be nominated to some of the TSDB's supported systems (refer to the TSC's *Watchlisting Guidance, March 2013*, § 3.14). Agents must coordinate with TREX to determine if a given individual falls within the limits of one of these exceptions.

11.4. (U) TSDB and Supported Systems

(U//FOUO) The TSDB supports federal, state, local, territorial, and tribal authorities and certain foreign governments' efforts to screen for KSTs through its exports. These authorities use their systems to run name checks against TSDB data. The TSC regularly provides updated subsets of TSDB data to several systems.

11.4.1. (U//FOUO) Known or Suspected Terrorist File (KST File)

(U) The KST file is maintained by the TSC and housed within the NCIC database. The KST file is composed of information related to the identities of individuals known or suspected to have knowingly engaged in conduct constituting, preparing for, in aid of, or related to, international or domestic terrorism or terrorist activities.

(U//FOUO) **Note:** The KST file was formerly known as the Violent Gang and Terrorist Organization File (VGTOF). The VGTOF was split into two separate files in August 2009: the Gang file and the KST file.

11.4.1.1. (U//FOUO) KST Handling Codes

(U//FOUO) Each record in the KST file must be assigned a handling code, as follows:

11.4.1.1.1. (U) Handling Code 1

(U//FOUO) Handling Code 1 is for individuals for whom there is an active federal arrest warrant in the NCIC Wanted Persons File. The warrant number must be included within the watchlist request. If a subject is watchlisted with Handling Code 1 and the arrest warrant becomes invalid, the case agent must submit a new watchlist request form to TREX to update the record. The following banner appears in the KST file when a Handling Code 1 is encountered:

LAW ENFORCEMENT SENSITIVE INFORMATION

WARNING - APPROACH WITH CAUTION

THIS INDIVIDUAL IS ASSOCIATED WITH TERRORISM AND IS THE SUBJECT OF AN ARREST WARRANT, ALTHOUGH THE WARRANT MAY NOT BE RETRIEVABLE VIA THE SEARCHED IDENTIFIERS. IF AN ARREST WARRANT FOR THE INDIVIDUAL IS RETURNED IN YOUR SEARCH OF NCIC, DETAIN THE INDIVIDUAL PURSUANT TO YOUR DEPARTMENT'S PROCEDURES FOR HANDLING AN OUTSTANDING WARRANT, AND IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER (TSC) AT (866) 872-9001 FOR ADDITIONAL DIRECTION.

IF AN ARREST WARRANT FOR THE INDIVIDUAL IS NOT RETURNED, USE CAUTION AND IMMEDIATELY CONTACT THE TSC AT (866) 872-9001 FOR ADDITIONAL DIRECTION WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.

UNAUTHORIZED DISCLOSURE OF TERRORIST WATCHLIST INFORMATION IS PROHIBITED. DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST. INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY THAT MAY NOT BE DISSEMINATED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

LAW ENFORCEMENT SENSITIVE INFORMATION

(U//FOUO) Whenever a Handling Code 1 subject is arrested, the case agent must modify the KST/NCIC record to change Handling Code 1 to Handling Code 3.

11.4.1.1.2. (U) Handling Code 2

(U//FOUO) Handling Code 2 is for individuals for whom DHS has issued, or will issue, a detainer if the individual is encountered by law enforcement. It may also be used for individuals for whom there is a sealed arrest warrant, and time is required to have the warrant unsealed (refer to subsection 11.9). A review of intelligence records must precede nominations of individuals into the KST file with this handling code. To use Handling Code 2, a review and approval for legal sufficiency by both the CDC and the OGC are required. The TSC Law Unit, in coordination with the NSLB, will provide such approval for OGC. The following banner appears in the KST file when a Handling Code 2 is encountered:

LAW ENFORCEMENT SENSITIVE INFORMATION*

WARNING - APPROACH WITH CAUTION

THIS INDIVIDUAL IS OF INVESTIGATIVE INTEREST TO LAW ENFORCEMENT REGARDING ASSOCIATION WITH TERRORISM AND THERE MAY BE A DETAINER AVAILABLE FROM THE DEPARTMENT OF HOMELAND SECURITY FOR THIS INDIVIDUAL.

IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER (TSC) AT (866) 872-9001 OR, IF YOU ARE A BORDER PATROL OFFICER, IMMEDIATELY CALL THE NTC TO ASCERTAIN IF A DETAINER IS AVAILABLE FOR THE INDIVIDUAL AND TO OBTAIN ADDITIONAL DIRECTION. PLEASE QUESTION THIS INDIVIDUAL TO ASSIST THE TSC IN DETERMINING WHETHER THE INDIVIDUAL ENCOUNTERED IS THE SUBJECT OF A DETAINER WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER.

UNAUTHORIZED DISCLOSURE OF TERRORIST WATCHLIST INFORMATION IS PROHIBITED. DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST. INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY THAT MAY NOT BE DISSEMINATED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

LAW ENFORCEMENT SENSITIVE INFORMATION

11.4.1.1.3. (U) Handling Code 3

(U//FOUO) Handling Code 3 is for individuals who have been watchlisted, but do not meet the additional criteria for Handling Code 1 or 2. These records must contain a first name, last name, and year of birth.[3] The following banner appears in the KST file when a Handling Code 3 is encountered:

LAW ENFORCEMENT SENSITIVE INFORMATION

DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST.

CONTACT THE TERRORIST SCREENING CENTER (TSC) AT (866) 872-9001 DURING THIS ENCOUNTER. IF THIS WOULD EXTEND THE SCOPE OR DURATION OF THE ENCOUNTER, CONTACT THE TSC IMMEDIATELY THEREAFTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.

[3] (U//FOUO) In some exigent circumstances, a circa date of birth may be acceptable. Case agents must coordinate with TREX.

ATTEMPT TO OBTAIN SUFFICIENT IDENTIFYING INFORMATION DURING THE ENCOUNTER, WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER, TO ASSIST THE TSC IN DETERMINING WHETHER OR NOT THE NAME OR IDENTIFIER(S) YOU QUERIED BELONGS TO AN INDIVIDUAL IDENTIFIED AS HAVING POSSIBLE TIES WITH TERRORISM.

DO NOT DETAIN OR ARREST THIS INDIVIDUAL UNLESS THERE IS EVIDENCE OF A VIOLATION OF FEDERAL, STATE OR LOCAL STATUTES.

UNAUTHORIZED DISCLOSURE IS PROHIBITED.

INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

WARNING - APPROACH WITH CAUTION

LAW ENFORCEMENT SENSITIVE INFORMATION

11.4.1.1.4. (U) Handling Code 4

(U//FOUO) Handling Code 4 is for individuals who have been designated Military Detainees (MILDETs). These individuals have been vetted by the Department of Defense (DOD) as persons detained by Coalition Forces in Afghanistan, Iraq, or Guantanamo Bay and have been shown to have no known nexus to terrorism. These records must contain a first name, last name, and year of birth. The following banner appears when a Handling Code 4 is encountered:

***MESSAGE KEY QWT SEARCHES ALL NCIC PERSONS FILES WITHOUT LIMITATIONS

LAW ENFORCEMENT SENSITIVE INFORMATION

DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE CONSIDERED A PERSON WHO MAY POSE A THREAT TO NATIONAL SECURITY.

CONTACT THE FEDERAL BUREAU OF INVESTIGATION (FBI) AT (866) 872-9001 DURING THIS ENCOUNTER. IF THIS WOULD EXTEND THE SCOPE OR DURATION OF THE ENCOUNTER, CONTACT THE FBI IMMEDIATELY THEREAFTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.

ATTEMPT TO OBTAIN SUFFICIENT IDENTIFYING INFORMATION DURING THE ENCOUNTER, WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER, TO ASSIST THE FBI IN DETERMING WHETHER OR NOT THE NAME OR IDENTIFIER(S) YOU QUERIED BELONGS TO AN INDIVIDUAL IDENTIFIED AS A FORMER MILITARY DETAINEE.

DO NOT DETAIN OR ARREST THIS INDIVIDUAL UNLESS THERE IS EVIDENCE OF A VIOLATION OF FEDERAL, STATE, OR LOCAL STATUTE(S).

UNAUTHORIZED DISCLOSURE IS PROHIBITED.

INFORMATION THAT THIS INDIVIDUAL MAY BE A PERSON WHO MAY POSE A THREAT TO NATIONAL SECURITY IS THE PROPERTY OF THE FBI AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE FBI.

11.4.1.2. (U) Silent Hit Nominations

(S//NF) Investigators may mark a subject's KST file entry as "silent," which will prevent any NCIC query from returning a KST record. For example, if during a routine traffic stop, local law enforcement queries a subject's name that has been identified as a silent hit, the officer will receive all criminal records for the subject that are in NCIC, but will not be notified that the subject is a suspected terrorist. In order to enter a subject's record as a silent hit, the nominating official must articulate a specific, narrowly defined, and legitimate operational justification. Possible justifications for a silent hit (with the requisite, written articulation) may include the following:

- (S//NF) The subject of the investigation is the target of 24-hours-a-day, seven-days-a-week (24/7) physical surveillance, undercover activities and operations, and/or sensitive source operations.
- (S//NF) The subject is an employee of, a member of, or affiliated with, a military, federal, state, local, or other law enforcement agency or any group that may have access to NCIC terminals.
- (S//NF) Other unique operational circumstances in which a nominating official can articulate a reasonable and detailed justification why the subject needs to be included as a silent hit.

(U//FOUO) Because a silent hit raises officer safety issues, subjects who are violent or are known to be armed and dangerous may not be marked as silent hits.

(U//FOUO) Other than at a primary screening by CBP and in NCIC, subjects marked as silent hits are not "silent" in any other watchlisting-supported systems. Requests for silent hits during a secondary screening by CBP can be coordinated on an investigation-by-investigation basis for USPERs through the TSC (refer to subsection 11.4.6.1 for further information).

11.4.2. (U) General Transportation Security Administration (TSA) Watchlisting Guidelines

(U//FOUO) The watchlisting community has developed five general guidelines regarding the inclusion of an individual on the TSA's No Fly and Selectee Lists that are necessary to effectively implement the No Fly List and Selectee List criteria.

(U) The five general guidelines are:[4]

[4] (U) This section contains Sensitive Security Information (SSI) that is controlled under 49 CFR Parts 15 and 1520. No part of this material may be disclosed to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For USG agencies, public disclosure is governed by 5 U.S.C. § 552 and 49 CFR Parts 15 and 1520.

1. (U//SSI) When evaluating the significance, relevance, and validity of a threat, careful consideration should be given to the extent to which the threat is current, specific, and credible.
2. (U//SSI) The Selectee List is not a default position for those who do not qualify for inclusion on the No Fly List and has distinct elements that must be met before an individual may be included.
3. (U//SSI) The purpose of the No Fly List is to protect against acts of terrorism; inclusion on the No Fly List has consequences that are operational, legal, economic, and diplomatic.
4. (U//SSI) Except for expedited nominations in accordance with watchlisting guidance, the decision to include a person on the No Fly List or Selectee List must include substantive derogatory information (refer to subsections 11.4.3. and 11.4.4. of this PG) that satisfies the criteria and justifies inclusion on either list. In investigations where nominations contain no substantive derogatory information or contain insufficient substantive derogatory information or insufficient identifying criteria, the individual will not be included on either the No Fly List or Selectee List.
5. (U//SSI) In accordance with watchlisting guidance, the White House may, on a temporary basis, direct the TSC to place categories of individuals who do not meet the established criteria on the No Fly List or the Selectee List, when necessitated by exigent circumstances, in response to credible intelligence information or a particular threat stream.
6. (U//SSI) Under exigent operational circumstances, when derogatory information may not be widely disseminated or stored in TIDE, individual watchlist status determinations can be made by the Director of the TSC, in accordance with the relevant criteria.

11.4.3. (U) TSA No Fly List

(U//FOUO) The TSA No Fly List is intended to prevent potential terrorists from boarding any commercial aircraft traveling within, to, or through U.S. airspace, or from boarding any U.S. flag carrier regardless of origination or destination. Inclusion does not provide grounds for arrest, detention, seizure of property or documents, or referral to a foreign government for comparable action. Inclusion also does not alter the fundamental right of U.S. citizens to return to the United States. FBI employees may not state or imply to watchlisted individuals that their ability to board an aircraft or return to the United States is contingent upon their cooperation with the FBI or USG (refer to [redacted]).

(U//SSI) Individuals, regardless of citizenship, who pose any of the following threats, may be placed on the TSA No Fly List:

- (U//SSI) A threat of committing an act of "international terrorism" or "domestic terrorism" (as defined in 18 U.S.C. § 2331), with respect to an aircraft (including a threat of air piracy or a threat to airline, passenger, or civil aviation security); or

- (U//SSI) A threat of committing an act of "domestic terrorism" (as defined in 18 U.S.C. § 2331(5)), with respect to the homeland, or
- (U//SSI) A threat of committing an act of "international terrorism" (as defined in 18 U.S.C. § 2331(1)) against any USG facility abroad and associated or supporting personnel, including U.S. embassies, consulates and missions, military installations (as defined by 10 U.S.C. § 2801(c)(4)) U.S. ships, U.S. aircraft, or other auxiliary craft owned or leased by the USG, or
- (U//SSI) A threat of conducting or engaging in a violent act of terrorism and who is operationally capable of doing so.

(U//SSI) An individual is "operationally capable" if, based on credible intelligence, he or she, acting individually or in concert with others, reasonably appears to have the ability, knowledge, opportunity, and intent or is actively seeking the opportunity to engage in a violent act of terrorism, consistent with 18 U.S.C. § 2331 or 18 U.S.C. § 2332b. For example, attempting to obtain an improvised explosive device (IED) would indicate an individual is operationally capable of committing an act of terrorism. However, simply conducting research concerning IEDs would not alone be sufficient without additional activity. Depending on circumstances and in combination with other facts, scouting potential targets or traveling for no legitimate purpose to places that have terrorist training grounds, regardless of whether the person is presently capable of using an IED, might also indicate an individual is operationally capable of committing an act of terrorism.

(U//SSI) In determining whether an individual is "operationally capable," consideration should be given to the following possible indicators regarding ability, knowledge, opportunity and/or intent:

- (U//SSI) The subject has undergone terrorist training or been provided some instruction, including receiving military training by a designated terrorism group.
- (U//SSI) The subject has indicated his or her intent to participate in planning or conducting an attack;
- (U//SSI) The subject has expressed a desire to martyr himself or herself;
- (U//SSI) The subject is in repeated contact with a known terrorist facilitator who recruits or facilitates travel of operatives;
- (U//SSI) The subject is planning an attack either alone or as part of a group; or
- (U//SSI) The subject is associated with a terrorist group or cell and is accumulating weapons or explosives.

(U//FOUO) Generally, in order to be included on the No Fly or Selectee List (detailed below), two preconditions must both be met:

1. (U//FOUO) Minimum identifying biographic criteria consisting of first name, last name, and full date of birth are required.
2. (U//FOUO) Minimum substantive derogatory criteria for inclusion must be met.

(U//FOUO) Upon receipt of threat information meeting the criteria described above, the assigned FBI case agent, in consultation with CTD, must determine whether the subject(s) of the investigation qualifies for the No Fly List. If the case agent determines that the subject qualifies, the watchlist request must be submitted to TREX within 24 hours of such a determination. TSA subject matter experts assigned to the TSC review all nominations to the No Fly List, and TSC may deny a subject's addition or removal from the list if it is determined the individual does not meet the above criteria.

11.4.4. (U//FOUO) TSA Selectee List

(U//SSI) The TSA Selectee List is intended to prevent a potential terrorist from passing through a TSA checkpoint without receiving a secondary screening. The screening offered by selectee status is solely to search for weapons and other dangerous items prior to boarding an aircraft. It is not a search designed to gain additional information through pocket litter, address books, and the like. An individual who does not meet the criteria for inclusion on the No Fly List, regardless of citizenship, may be listed as a TSA selectee if the individual is both:[5]

1. (U//SSI) A member of a foreign or domestic terrorist organization (including a "foreign terrorist organization" designated pursuant to statute or executive order).
2. (U//SSI) Associated with "terrorist activity" (as such term is defined in subsection 212(a)(3)(B) of the Immigration and Nationality Act [8 U.S.C. 1182(a)(3)(B)]), unless information exists that demonstrates that the application of a secondary screening to such a person is not necessary, in which case such persons may be excluded from the Selectee List.

(U//FOUO) Subject matter experts assigned to the TSC determine if individuals nominated as selectees meet the criteria for this list. TSA personnel regularly review selectees and may upgrade or remove a subject from the Selectee List if current intelligence shows that the subject either meets or does not meet criteria 1 and 2, as listed above. TSC and/or TREX will notify the case agent of any changes to the selectee status of the subject.

(U//FOUO) The minimum biographical information needed to nominate an individual to the Selectee List is the first name, last name, and full date of birth.

11.4.5. (U//FOUO) Consular Lookout and Support System (CLASS)

(U//FOUO) Subjects may be included in the DOS's CLASS database. CLASS has two subsystems: CLASS-Visa and CLASS-Passport. CLASS-Visa is used by DOS to screen non-USPERs applying for visas to enter the United States (USPERs are not included in CLASS-Visa). CLASS-Passport is used by DOS to screen USPERs applying for U.S. passports.

11.4.6. (U//FOUO) TECS System

(U//FOUO) Individuals may be included in the DHS TECS system, which serves as the primary integrated lookout system currently available at U.S. ports of entry. DHS uses TECS to screen

[5] (U) For additional information, please see TSC's 2013 Watchlist Guidance, § 3.11.2.

both USPERs and non-USPERs. CBP inspectors query TECS when an individual seeks to enter the United States.

11.4.6.1. (U//LES) T7 (Silent Hit)

(U//LES) For operational needs, there is an exclusion code in TECS called a T7 (Silent Hit) that can be placed on a KST record for a passenger who matches against the TSDB. Use of this code will make the watchlist information invisible to a CBP officer at the port of entry (POE Primary), and thus prevent the passenger's referral to secondary screening. To designate a record for a silent hit, TSC may advise the case agent during the encounter management process of the T7 designator and its criteria and seek concurrence from the case agent to designate the subject as a T7. If the case agent agrees, the agent will be required to complete an FD-930 to modify the subject's watchlist status. After the subject has been changed to a T7, the TSC will advise CBP, via established channels, of the watchlist status change. The criteria for designation of a passenger as a T7 are:

- (U//LES) Be the current subject of an FBI counterterrorism investigation
- (U//LES) Is not on either the TSA No Fly or the TSA Selectee lists
- (U//LES) Not be flagged in NCIC as "Armed and Dangerous," "Violent Tendencies," "Explosives Expertise," "Suicidal," or "Martial Arts Experts"
- (U//LES) Does not pose a threat to officer safety
- (U//LES) Be a United States Person (USPER)

11.4.7. (U//FOUO) TIPOFF United States-Canada (TUSCAN)

(U//FOUO) Non-USPER investigative subjects may be entered into TUSCAN, a program based on a United States/Canadian agreement through which sensitive but unclassified biographic lookout data elements on a subject are shared with the Canadian government. Derogatory information is also transferred to the Canadian government on an investigation-by-investigation basis. Canadian citizens are not included in TUSCAN. USPERs are not included in TUSCAN unless they are on the No Fly or Selectee Lists or have an active federal arrest warrant.

11.4.8. (U//FOUO) TIPOFF Australian Counterterrorism Information Control System (TACTICS)

(U//FOUO) Non-USPER investigative subjects may be entered into TACTICS, a program based on a United States/Australian agreement, through which sensitive but unclassified biographic lookout data elements on the subject are shared with the Australian government. Derogatory information is also transferred to the Australian government on an investigation-by-investigation basis. Australian citizens and permanent residents from Australia, with the exception of those who hold dual U.S. citizenship, are included in TACTICS. USPERs are not included in TACTICS unless they are on the No Fly or Selectee Lists or have an active federal arrest warrant.

11.4.9. (U) Additional Supported Systems

(U//FOUO) The TSC, through the TSDB, also makes terrorist identifiers accessible to other entities through the regular export of updated subsets of TSDB data. These include:

- **(U//FOUO) Other supported databases.** The TSC also provides the FBI and certain other federal authorities with access to TSDB information for screening or analytical purposes. This may include access to the FBI's central recordkeeping system, the FTTTF database, and the TSA's Office of Transportation Threat Assessment database.
- **(U//FOUO) Certain foreign governments.** The TSC provides a subset of the TSDB to certain foreign partners in exchange for their terrorism screening information.

11.5. (U) CTD Nomination Policy

(U//FOUO) Case agents must submit watchlist nominations to TREX for all subjects of 266 or 415 investigations, in accordance with subsection 11.6, with the exception of investigations predicated on a victim, organization, activity, or comparable unidentified entity for which watchlisting is ineffective. Subjects of other CTD-managed investigative classifications should generally be reclassified to 266 or 415 investigations if there is reason to believe the subjects meet the watchlisting standard (refer to subsection 11.3.). Predicated CT subjects not opened as 266 or 415 subjects may be considered for watchlisting on a case-by-case basis, but in all circumstances must meet the watchlisting standard.

(U//FOUO) Subject matter experts at TREX must evaluate each nomination to ensure the watchlisting standard has been met and sufficient identifying information is available. TREX must notify and provide guidance to FOs, by e-mail, of subjects who will not be submitted to the watchlist.

11.6. (U) Watchlisting Submission Standards

11.6.1. (U) Subject Nomination

(U//FOUO) Case agents must nominate individuals for inclusion in the TSDB, as required by the nomination policy for the applicable investigative program, by submitting a watchlist request, in accordance with subsection 11.7. of this PG. A case agent is responsible for ensuring the request is submitted in accordance with the timelines established herein. The request must be submitted within **three business days** of the date created in FBI's central recordkeeping system to open the investigation. Nominations will include all available subject identifiers, to include photographs or other available biometric information. If the subject is being nominated to the TSA No Fly List, he or she must be submitted by the nominating official within **24 hours** of receipt of information that qualifies the subject for the No Fly List. TREX must process No Fly List upgrades within **24 hours** of receipt.

(U//FOUO) If there is a determination, due to an exigent circumstance or CTD's direction, that the nomination needs to be submitted more quickly, FOs must contact TREX directly by telephone and submit the watchlist request, in accordance with subsection 11.7. of this PG.

(U//FOUO) **Note:** For CTD purposes in regard to watchlisting, an exigent circumstance is an emergency situation requiring swift action to prevent danger to life or serious damage to property.

(U//FOUO) Domestic terrorism investigations focused on militia extremists, white supremacist extremists, and sovereign citizen extremists often have identified active links to law enforcement officers and those in positions to check NCIC for warrants. Subjects of these investigations must be watchlisted, but an individual may be entered into the KST file as a silent hit, in accordance with subsection 11.4.1.2. of this PG. Operational concerns regarding watchlisting a specific DT subject need to be coordinated between the FO, the CTD program management unit, and TREX.

(U//FOUO) When the FBI opens an investigation and the subject has already been watchlisted by another agency, a case agent must submit a watchlist nomination request within **three business days** of the date created in the FBI's central recordkeeping system to open the investigation. The request will enhance the Terrorist Identities Datamart Environment (TIDE) record and will document the FBI's investigative interest in the subject. Failure to submit the watchlist request when another agency has nominated the individual to the TSDB could result in removal of an FBI subject from the watchlist without notification to the FBI. This process ensures that the USIC has all available information if the original nominating agency attempts to remove the subject from the watchlist.

(U//FOUO) **Note:** As a best practice, if sufficient information is known to support watchlisting when the investigation is opened, the watchlist request should be prepared and submitted at the time the investigation is opened.

(U//FOUO) TREX must process nominations within **five business days** of receiving the watchlist request.

11.6.2. (U) Subject Modification

(U//FOUO) After the initial submission, the nominating official must update the watchlist request information (e.g., updated derogatory information that may result in a change of watchlisting status, change in investigation, biographical information, or the nominating official's contact information) as soon as new information becomes available. Additional identifiers must be forwarded to TREX using the watchlist request's modify feature. Supervisors are required to review the investigative file for new identifiers during the 90-day file review for all terrorism investigations. When adding, modifying, or deleting data from a specific record, only the subject's name, sex, race, date of birth, and new or changed information is required on the watchlist request. Other information that has previously been submitted need not be reentered.

(U//FOUO) Modifications may add or delete information from an existing record and/or upgrade or downgrade a subject's watchlisting status. If a modification is warranted, a watchlist request must be submitted, in accordance with subsection 11.7. of this PG, by the originating FO. Such information must be submitted to TREX in a timely manner, not to exceed **three business days** from the day the new information is serialized into the FBI's central recordkeeping system or the day the determination is made to change a subject's status, absent any exigent circumstance or other direction from CTD. If exigent circumstances exist or CTD directs, FOs must contact

TREX directly, via telephone, and submit watchlist requests, in accordance with subsection 11.7. of this PG.

(U//FOUO) TREX must subsequently process modifications within seven **business days** of receipt of the watchlist request.

(U//FOUO) Modifications to upgrade a subject to the TSA No Fly List must be submitted by the nominating official within **24 hours** of receipt of information that qualifies the subject for the No Fly List. TREX must process No Fly List upgrades within **24 hours** of receipt. After the arrest of a Handling Code 1 subject, the nominating official must submit a watchlist request to TREX within three business days of the case agent learning of the subject's arrest.

(U//FOUO) If a subject who has been watchlisted moves to another FO's jurisdiction, the subject must remain watchlisted until the receiving office opens an investigation, unless the watchlisting standard is no longer met. The closing FO must set a lead for the receiving FO, notifying it of the subject's relocation and requesting it to open an investigation. The receiving FO must submit a watchlist request for each subject, updating the TSDB record with the new file number, case agent's name, and any additional identifiers (such as the subject's address and driver's license number) resulting from the move. The receiving FO must submit the watchlist modification request within three business days of the date created in the FBI's central recordkeeping system to open the investigation. If the receiving FO believes an investigation is not warranted, the matter must be referred to CTD, in accordance with subsection 4.10. of this PG.

(U//FOUO) A watchlisted subject who moves outside the United States and continues to meet the watchlisting standard must remain in the TSDB as long as an FBI investigation remains open.

11.6.3. (U) Subject Removal

(U//FOUO) When a predicated IT or DT investigation is closed, a request for removal of any watchlisted subjects must be submitted, absent the criteria set forth in subsections 11.10. or 11.11. of this PG.

(U//FOUO) Upon closing an investigation (i.e., a PI or a full investigation) that has a watchlisted subject, a removal request must be submitted, in accordance with subsection 11.7. of this PG, within **three business days** of the written approval and notification to CTD of the investigation's closure. The three-business-day timeline starts on the closing date shown in the FBI's central recordkeeping system and stops when TREX receives a completed removal package.

(U//FOUO) If an exigent circumstances exist or CTD directs, FOs must contact TREX directly via telephone and submit watchlist requests in accordance with subsection 11.7. of this PG.

(U//FOUO) TREX must process removals within **five business days** of receiving the watchlist request.

(U//FOUO) If a subject permanently moves abroad, with no known return date to the United States, and a determination is made to close the investigation, the FO must submit a watchlist removal request to TREX, as provided above. If, however, the FO or the CTD program management unit determines removal of the subject is not warranted because the investigation is not complete, and the subject continues to be reasonably suspected of being involved in terrorism

or terrorist activities, then watchlisting oversight needs to reside with the FBI. Refer to subsection 11.11 of this PG and submit a watchlist modification request annotating the individual as a nonsubject, watchlisted person.

11.7. (U) Watchlist Request Submission Process and Guidance

(U//FOUO) FO supervisors are responsible for ensuring a watchlist request and the accompanying EC are: (1) submitted to TREX within the established time frames detailed in subsection 11.11 of this PG, (2) the nomination package contains sufficient derogatory information to establish the subject meets the watchlisting standard, and (3) the identifiers listed on the watchlist request and EC are accurate. Supervisors are reminded that the automated 90-day file review printout includes a section where SSAs confirm that all watchlisting identifiers have been submitted to TREX. This includes submitting a JPEG (Joint Photographic Experts Group)-formatted photograph of the subject (e.g., a DMV photograph or a photograph from another source).

(U//FOUO) TREX must review the watchlist requests to verify and validate all submissions, then process any watchlist requests to facilitate watchlisting, if necessary.

(U//FOUO) All watchlist requests, with their supporting ECs, must be submitted to TREX via the TREX FD-930 Database. A watchlist request must be accompanied by a supporting EC, with an appropriate action lead to TREX. In the event of an incomplete request, TREX must notify the FO to resubmit the missing element(s).

- (U//FOUO) IT Program: TREX must verify and validate watchlist requests to ensure they meet the watchlisting standard (refer to subsection 11.3.). TREX will forward all requests to NCTC for inclusion in TIDE. NCTC will in turn export those identifiers that meet the watchlisting standard to the TSC for inclusion in the TSDB and appropriate, supported systems.
- (U//FOUO) DT Program: TREX must verify and validate watchlist requests and will only forward subjects who meet the watchlisting standard to TSC for inclusion in the TSDB and appropriate, supported systems. If the watchlisting standard is not met for a nomination, TREX must notify and provide guidance to the submitting FO.

(U//FOUO) The supporting EC must contain a short, plain description of the investigation, including the terrorist group with which the subject is associated and the type of involvement (e.g., financier, facilitator, trainer, or operator). IT Program watchlist requests validated by TREX may be reviewed by anyone with access to TIDE, including OGA personnel. The request must not include information pertaining to FISA collection, No Foreign (NF) or Originator Control (OC) dissemination controls, "protect identity" individuals, Bank Secrecy Act information, Suspicious Activity Report (SAR) and Currency Transaction Report (CTR) information, or information obtained utilizing grand jury subpoenas. Such information may be included, but clearly marked, in the accompanying EC if it is necessary to support the justification for watchlisting. FISA-obtained or FISA-derived identifiers must also be portion marked accordingly so that they can be accurately delineated in TIDE.

(U//FOUO) If the supporting documentation is not yet serialized into the FBI's central recordkeeping system at the time the watchlist request is submitted, copies must be attached to the request. This procedure ensures there is no delay in the initial submission, modification, or removal.

11.7.1. (U) Subject Identification

(U//FOUO) Nominations to the TSDB must include:

1. (U) Last name

 AND

2. (U) One or more of following:
 - First name
 - Complete date of birth
 - Passport number
 - Alien registration number
 - Visa number
 - Social security number
 - Other unique identifying number
 - Telephone number (unclassified only)
 - E-mail address (unclassified only)
 - License plate number

 OR

3. (U) Two or more of the following:
 - Country of citizenship, if different from place of birth
 - Place of birth (city or country), if different from country of citizenship
 - Circa or partial date of birth (partial [e.g., 1960]; or range [e.g., 1960-1965])
 - Full name of an immediate family member (e.g., parent, spouse, sibling, or child)
 - Occupation or current employer
 - Specific degrees received
 - Schools attended
 - Physical identifiers, such as race, height, or weight
 - Unique physical identifiers, such as scars, marks, or tattoos
 - Street address or other sufficiently specific location information

(U//FOUO) The watchlist request and/or accompanying EC must contain all the known identifying information on the individual, even if it exceeds the minimum specified above. This may also include photographs, fingerprints, or other biometric data. Furthermore, all available identifiers must be submitted to the TSDB either on the initial request or on a subsequent

modification request. In limited circumstances validated by TREX, an individual may be nominated to the TSDB with only partial identifiers.[6]

(U//FOUO) Prior to any initial nomination, modification, or removal, the case agent and supervisor must review and address the following issues:

- (U//FOUO) The inclusion, accuracy, and completeness of possible identifiers.
- (U//FOUO) The appropriateness of the designated handling code.
- (U//FOUO) The inclusion of statements that the subject is "Armed and Dangerous" or has "Violent Tendencies," as appropriate.
- (U//FOUO) The inclusion of any active federal warrant(s) for the subject. If so, the case agent/supervisor must ensure that the entry request is for a Handling Code 1 and must provide the warrant number.
- (U//FOUO) The inclusion of a statement that all necessary/known cautions and medical conditions have been requested/identified, as appropriate.
- (U//FOUO) The accuracy of the investigative file number.
- (U//FOUO) If the submission requests an exclusion from a particular watchlist, the exclusion must include statements in the watchlist request and corresponding EC, justifying the exclusion.
- (U//FOUO) The submission of photographs for each subject, which must be scanned into a JPEG format and provided to TREX.

11.8. (U) Expedited Nominations

(U//FOUO) Expedited nominations are available if exigent circumstances exist for entry into the TSDB. In the event a subject's watchlisting requires expediting (e.g., subject travel is imminent), the nomination must be submitted to TREX (during business hours) or to the Terrorist Screening Operations Center Watch (outside normal business hours), which will conduct appropriate coordination with the NCTC and/or within TSC. Expedited nominations must still meet the criteria for entry in the TSDB. The TSC will make a final determination if the subject qualifies for the TSDB, including the TSA No Fly List or Selectee List. In addition to the TSA lists, the subject's record will be exported to all appropriate supported screening systems.

(U//FOUO) All expedited nominations must be submitted in accordance with subsection 11.7. of this PG and be processed immediately by TREX, with subsequent submission to the TSC. Any supporting documentation necessary to meet the normal watchlisting requirements that was not provided in the original expedited request must be provided to TREX on the next business day. The TSC must remove the expedited record from the TSDB and all supported systems within 72

[6] (U//FOUO) An inability to validate a nomination for inclusion in the TSDB does not always prevent sharing information with NCTC for possible inclusion within its TIDE database, as TIDE has a greater ability to accept partial or fragmentary information.

hours, unless the nominating official forwards sufficient derogatory information through the routine process.

11.9. (U) Arrest Warrants and Interpol Notices for Watchlisted Individuals

(U//FOUO) If an active federal arrest warrant exists in the NCIC Wanted Persons File for a terrorism subject, the case agent must submit a watchlist request for nomination to Handling Code 1. The documenting EC and request must include the NCIC warrant number (Wanted Persons File record number). In the investigation of a currently watchlisted individual, this documentation must include all descriptive, biographical, or cautionary information about the subject that has not already been entered in the TSDB. TREX will review the submitted information and forward it to the NCTC for entry into TIDE or directly to the TSC, as appropriate.

(U//FOUO) If subsequent to entry as a Handling Code 1, the federal arrest warrant ceases to be active in the NCIC Wanted Persons File (e.g., the arrest warrant has been served or recalled by the court), the FO must submit a notification EC and watchlist modification request within three business days to change the subject to Handling Code 3. TREX must submit the modification to NCTC for entry into TIDE or directly to the TSC, as appropriate.

(U//FOUO) In rare circumstances, such as a sealed federal indictment where a subject may not have a Wanted Person File record number in NCIC, it may be necessary to keep information concerning a pending federal arrest warrant out of the TSDB. In such circumstances, the notification EC concerning the warrant must provide a reasonable and detailed justification for the exclusion (refer to subsection 11.14. of this PG). If encountered by law enforcement, and in order to ensure that the subject is detained long enough to allow the indictment to be unsealed and an arrest warrant issued and served, such subjects need to be watchlisted as a Handling Code 2 (refer to subsection 11.4.1.1. of this PG).

(U//FOUO) If an active federal arrest warrant exists for the subject, absent sensitive circumstances, the case agent may apply for an Interpol Red Notice. Interpol publishes these notices to member states so that if the subject is found, the subject can be arrested and extradited to the country holding the warrant.

(U//FOUO) If an Interpol Red Notice is filed, a watchlist modification request must be submitted to TREX with the Red Notice number.

11.10. (U) Subjects Arrested or Convicted of Terrorism-Related Offenses

(U//FOUO) All known terrorists must remain watchlisted (refer to Appendix A of this PG for a definition of "known terrorist"). If an FO closes an investigation of a known terrorist (e.g., after the criminal investigation has concluded), a modification must be submitted via the TREX FD-930 Database and the closing EC, with the justification details attached. TREX must then submit a request to modify the TSDB record, in accordance with subsection 11.11.1. of this PG.

(U//FOUO) If an individual is acquitted or charges are dismissed for a crime related to terrorism, the subject must be removed from the watchlist unless the subject continues to meet the watchlisting standard (refer to subsection 11.3.). Terrorism subjects convicted of nonterrorism

offenses must be removed from the watchlist unless the watchlisting standard continues to be met.

11.11. (U) Nonsubject Nominations

(U//FOUO) Typically, the FBI only nominates subjects of predicated investigations for watchlisting. However, certain circumstances may arise in which the FBI determines a person who is not the subject of a predicated investigation warrants watchlisting and meets the watchlisting standard (refer to subsection 11.3. of this PG). This may include, in limited circumstances, the subject of a closed FBI investigation.

(U//FOUO) This process to watchlist an individual may not be utilized based on hunches or suppositions. The nominating official must provide particularized derogatory information concerning the threat posed by nonsubjects who meet the watchlisting standard. In these matters, the FBI may only nominate an individual if both of the following criteria have been met:

1. (U//FOUO) The individual is not residing or permanently located in the United States.
2. (U//FOUO) The individual has been linked to the subject of an active IT or DT investigation, or the FBI otherwise possesses sufficient derogatory information to meet the standard for watchlisting.

(U//FOUO) FBI personnel deployed with DoD entities may not nominate subjects of military operations conducted under DoD authority. These individuals are nominated to the TSDB by DoD.

11.11.1. (U) Nonsubject Nomination Process

(U//FOUO) Any FO or Legat with information regarding a nonsubject meeting the above criteria (e.g., former subjects who have left the country or suspected terrorists identified by foreign governments) must submit information to TREX for watchlisting, in accordance with the following procedures.

(U//FOUO) The FO or Legat must submit all watchlist requests to TREX via the TREX FD-930 Database. A watchlist request must be accompanied by a supporting EC, with an appropriate action lead for TREX to assume responsibility for the watchlist record. In the event of an incomplete request, TREX must notify the FO or Legat to resubmit the missing element(s). If the individual is already watchlisted by another agency, TREX must submit an FD-930 to NCTC indicating FBI interest.

(U//FOUO) Submissions to TREX must be made in accordance with the timelines established in subsection 11.6. TREX will not nominate or take over watchlist responsibility if the FO provides insufficient information regarding the subject. TREX will notify the FO if current circumstances prevent watchlisting.

11.11.2. (U) Review of Nonsubject Records

(U//FOUO) Nonsubjects nominated to the TSDB are tracked by TSC, using the FD-930 Database. TSC is responsible for verifying and validating the watchlist status of USPER nonsubjects annually to ensure that the information is accurate and that intelligence reporting continues to suggest the USPER poses a national security risk related to terrorism that warrants

watchlisting. If TSC determines a nonsubject no longer meets the watchlisting standard, TSC must remove the nonsubject from the watchlist and notify the FO or Legat office that originally nominated the individual.

(U//FOUO) If a watchlisted nonsubject is encountered, the TSOU will follow normal notification procedures. On completion of the encounter, a copy of the TSOU log must be e-mailed to TREX for additional follow-up regarding the nonsubject's watchlist status. TREX must review the encounter details to ensure the individual meets the watchlisting standard and must modify the record with any new identifiers developed. If a nonsubject is encountered during travel within the United States, TREX will set a Guardian lead to the appropriate FO for appropriate local response. If, upon closure of the Guardian lead, the FO determines there is no nexus to terrorism, TREX will submit an FD-930 to remove the subject from the watchlist.

11.11.3. (U) Nonsubject Nomination from DOJ Components

(U//FOUO) On October 3, 2008, DOJ designated the FBI as the central watchlist nominator for all DOJ components. Information regarding known or suspected terrorists developed through other investigative arms of the DOJ (e.g., the ATF, the Drug Enforcement Administration [DEA], or the United States Marshals Service [USMS]) is passed at the FO level through established relationships with the FBI JTTF. The NJTTF or the CTD program management unit is the recipient of terrorism information when provided at the headquarters level. If the FBI does not open an investigation, but the individual(s) meets the nonsubject nomination criteria listed in subsection 11.11., the FBI recipient of this information must provide details to TREX, as described in subsection 11.11.1. TREX must ensure the individual(s) is properly watchlisted, in accordance with subsection 11.7.

(U//FOUO) If the United States National Central Bureau (USNCB) obtains terrorism-related intelligence, it will provide the intelligence to CTD, which will review the terrorism intelligence and will generate Guardian assessment leads for investigation, as appropriate. If a terrorism investigation is generated as a result of the Guardian lead, the subject will be submitted for watchlisting, in accordance with subsection 11.5. of this PG.

11.12. (U) Foreign Government Information (FGI)

(U//FOUO) Foreign governments occasionally provide information regarding non-USPER individuals who are under investigation in their countries for crimes related to terrorism or individuals who are reasonably suspected of engaging in terrorism or terrorist activity. Those receiving such specific derogatory information of only non-USPER individuals may submit these individuals for watchlisting. The receiving office must also seek and collect available identifiers and biometrics (e.g., photographs and fingerprints), as appropriate. If such FGI is provided through an established or formal sharing relationship between the United States and the foreign government, then reasonable suspicion is presumed. The reasonable suspicion standard, however, must be met when information is not received under an established, formal, or HSPD-6 sharing process.

(U//FOUO) When FGI is provided by a foreign agency with a terrorism screening information sharing or HSPD-6 arrangement with the TSC, Legat offices must determine if the FGI was provided by the partner agency pursuant to the arrangement. Each arrangement defines a unique

watchlisting standard that subjects submitted by the partner agency must meet, and the partner agency must designate the information as being submitted pursuant to the arrangement, as this is their indication that the information held on the subjects meets the standard outlined in the arrangement.

11.12.1. (U) Watchlisting of Criminal Justice Information Services (CJIS)-Derived Information

(U//FOUO) FGI provided to CJIS through a memorandum of cooperation or similar memorialized agreement establishing a formal information-sharing relationship with a foreign partner may be provided without particularized derogatory information directly to NCTC. CJIS provides the personal identifiers and biometrics of these individuals to the USIC as part of its HSPD-6 information-sharing responsibility. This is not an FBI nomination. FGI does not require an annual review, as CJIS requests updated information on a regular basis. CJIS must forward any updated identifiers it obtains to NCTC so the TIDE record may be updated and NCTC can determine whether continued watchlisting of the individual is necessary.

(U//FOUO) If a foreign government provides records that include a mixture of terrorism, criminal, or other information, CJIS must attempt to identify and separate records related to terrorism, as only terrorism records are included in TIDE and the TSDB. If CJIS cannot distinguish between the criminal, terrorism, and other categories of records, it may not submit the entire batch of records. In addition, information provided informally or on an ad hoc basis must not be forwarded to NCTC. Such records and any biometrics will remain a part of the larger CJIS biometric holdings and will remain available in the future to connect individuals to terrorism.

11.12.2. (U) Watchlisting of Legat-Derived Information

(U//FOUO) All Legat offices that have obtained FGI terrorist information must submit watchlist requests to TREX via the TREX FD-930 Database, unless provided pursuant to an HSPD-6 sharing arrangement with the TSC. A watchlist request must be accompanied by a supporting EC, with an appropriate action lead to TREX to assume responsibility for the watchlist record. In the event of an incomplete request, TREX must notify the Legat to resubmit the missing element(s). Upon receipt of the FGI from a Legat, TREX must review the information and submit a watchlist request to NCTC if the FGI meets the watchlisting standard. If an FGI-derived subject is encountered, the normal TSC encounter process must be followed. Any new identifying information must be provided to TREX, which will modify the subject's biographical information. TREX must set an information lead to the Legat regarding the new information.

(U//FOUO) FGI provided to Legat offices pursuant to terrorism screening information sharing or HSPD-6 arrangements with the TSC should be sent via EC to the designated POC within the TSC International Information-Sharing Program (IISP). The partner's original submission in Excel, Word, or other format as submitted by the partner should be attached or forwarded by expedited mail. Legat offices will be contacted periodically by IISP to assist in contacting the partner for updates to the information.

11.12.3. (U) FGI Submission Review Process

(U//FOUO) A terrorist's biographic information and photographs (described above in subsection 11.12.2. of this PG) that are provided by a foreign government must be sent to TREX and processed as FGI. TREX will provide this terrorist information to NCTC, along with an FD-930, if needed, in order to enter the individual into TIDE and the TSDB. TREX will not provide additional oversight or review of these FGI records, unless additional information is provided by the foreign government or an encounter occurs. If a Legat obtains additional identifiers, derogatory information, or reasons to remove FGI from TIDE, the new intelligence must be sent to TREX, which will forward this information to NCTC. The original recipient of FGI terrorism information must also provide fingerprints and biographic information to CJIS, if available.

11.13. (U) Watchlisting of Deceased Individuals

(U//FOUO) The TSDB may not include identity information of known or suspected terrorists who are confirmed dead, unless:

- (U//FOUO) There is information to support a reasonable suspicion that an existing known or suspected terrorist is using that identity information.
- (U//FOUO) A recognized terrorist organization collects known or suspected terrorist identity information for use by its members in preparing for or committing terrorist acts, **and** the travel documents related to the deceased known or suspected terrorist have not been recovered.

 (U//FOUO) **Note:** A classified list of recognized terrorist organizations that are known to reuse terrorist identity information is maintained on the NCTC Current site, available on the Sensitive Compartmented Information Operational Network (SCION).

11.14. (U) Exclusion from a Supported System

(U//FOUO) In rare circumstances, the subject of an investigation may be excluded from a particular watchlisting-supported system if a reasonable and detailed operational justification is provided. An FO that wishes to exclude a subject from a supported system must articulate the justification as part of the watchlist request and/or supporting EC.

> (U//FOUO) **Note:** The existence of local or state public disclosure laws are not sufficient justification for exclusion.

(U//FOUO) Subject matter experts in TREX will review justifications for exclusion from supported systems and determine whether the exclusion is warranted. TREX must notify the submitting FO if an exclusion is not warranted.

11.15. (U) Redress

(U//FOUO) Individuals may seek redress for travel delays and other inconveniences they experience due to screening and/or watchlist issues, real or perceived. An interagency *Memorandum of Understanding on Terrorist Watchlisting Redress Procedures* between the TSC, the FBI, and other relevant agencies is in place to address how each agency will respond to such requests for redress. As such, the TSC may request additional information directly from an FBI

FO or a Legat to respond to a request for redress. An FO or a Legat must provide the information requested by TSC within 30 days of the receipt of the request. After considering the available information, TSC makes the final determination as to whether the watchlist record will remain in the TSDB, be modified, or be removed.

11.16. (U) Inbound/Outbound Travel of Watchlisted Persons

(U//FOUO) If the FBI wants a watchlisted subject to have unimpeded travel through screening agencies at the U.S. border, advance coordination between the FO, the CTD program management unit, and the TSC must occur. The TSC maintains regular contact with other government agencies that manage and/or use the terrorism watchlists and is able to facilitate requests to avoid unnecessary delay and/or additional scrutiny of subjects for whom the FBI desires to allow unimpeded travel (e.g., significant public benefit parolees). FBI requests are subject to the concurrence of the screening agency and may not always be honored.

(U//FOUO) TSC may also authorize a one-time waiver to allow individuals on the No Fly List to fly into or out of the United States. The FO, Legat, and/or CTD program management unit must coordinate such requests with TSC's Operations Center. Refer to the TSOU Intranet site.

12. (U) Investigative Methods

(U//FOUO) This section is not intended to be an exhaustive discussion of all available investigative methods, but rather of those unique to counterterrorism investigations. For a more thorough discussion of all available investigative methods, refer to the DIOG.

12.1. (U) Name Traces

(U//FOUO) A name trace is a formal request to another government agency to conduct a search of existing records for information regarding a subject of interest. Requests for name traces are typically handled by the CTD program management unit. FOs wishing to run a name trace may send an EC with a lead to the program management unit, including the subject's predication and all available identifiers.

12.1.1. (U) Authorized Investigative Activity

(U//FOUO) Name traces are authorized in both the IT and DT Programs, at all levels of investigative activity.

12.1.2. (U//FOUO) CIA Name Traces

(U//FOUO) Requests to the CIA for general information are submitted electronically via the CIA External Name Trace System (CENTS). CENTS requests are handled by CIA's External Inquiries Branch (EIB), and CENTS can be accessed via the SCION system at the following address: [redacted] Trace requests are sent to CENTS if a subject is suspected of involvement in terrorism, but there is no known group or network with which the subject is affiliated.

(U//FOUO) If there is a known group affiliation, rather than using the CENTS system, CTD personnel will submit a trace request cable (refer to the CTD Templates Page) to the appropriate element that handles that group within CIA's Counterterrorism Center (CTC). CTC has access to some data that is not available to the EIB, which may provide a fuller trace response than what is available through CENTS. CTC will only conduct a trace of a subject who has a known group affiliation.

12.1.3. (U//FOUO) NSA Name Traces

(U//FOUO) Name trace requests to the NSA are also sometimes called requests for information (RFI). Legal constraints forbid NSA from conducting trace requests regarding USPERs. NSA also has special requirements regarding a citizen of a Five Eyes (FVEY) member country. Thus, it is important to know the nationality of the trace target and include it whenever possible. An NSA request can be made by one of two methods: (1) electronically, using NSA's Customer Gateway system or (2) via an EC.

1. (U//FOUO) **Gateway method**: An electronic request may be submitted through the Gateway system using the SCION system at [redacted]
2. (U//FOUO) **EC method**: An EC may also be used to submit the necessary information to the NSA's senior representative to the FBI, who will then forward the information to the

appropriate entities within NSA. An example of this EC can be found on NSA's Intranet site.

12.2. (U) Interviews

(U//FOUO) An interview is the questioning of an individual (including a subject) in a manner designed to gather information that is accurate, pertinent to, and within the scope of, an authorized assessment or predicated investigation. See DIOG Section 18.

(U//FOUO) For rules and standards on the conduct of interviews, refer to DIOG Section 18.

12.2.1. (U) Authorized Investigative Activity

(U//FOUO) Interviews are authorized in both the IT and DT Programs at all levels of investigative activity.

12.2.2. (U) Deconfliction

(U//FOUO) An FO must implement strong deconfliction measures prior to interviewing the subject of a predicated investigation to ensure the interview will not compromise investigations in other FOs or alert the subject's associates. Such deconfliction must be documented to the investigative file in advance of the interview. A copy must also be provided to the CTD program management unit. The deconfliction documentation must address the following issues:

- (U//FOUO) The name(s) and investigative file number(s) of any FBI subject(s) known to be in contact (e.g., personal, telephonic, or e-mail) with the subject of the interview.
- (U//FOUO) The name(s) of any individual(s) of significant interest (e.g., a known or suspected terrorist abroad who is not the subject of an FBI investigation) known to be in contact with the subject of the interview.
- (U//FOUO) The frequency of contact and the date of the last contact for each individual in one of the above groups known to be in contact with the subject of the interview.
- (U//FOUO) The steps taken to coordinate with other FOs, Legats, and/or USIC, federal, state, local, or foreign partners whose investigative equities may be impacted by a planned interview.
- (U//FOUO) An analysis of the potential for an individual in contact with the subject of the interview to be alerted to possible FBI investigative interest.
- (U//FOUO) A synopsis of the general interview approach strategy (e.g., a follow-up on a secondary screening by CBP or a possible offer to become a CHS) and any false purpose or nondisclosure of FBI affiliation that is planned.
- (U//FOUO) What, if any, information from sensitive sources (e.g., FISA or a singular CHS) has been used to formulate the interview questions, and what steps are being taken to protect the sensitive source.

12.3.5. (U) Sensitive Financial Traces

(S//NF) Sensitive CIA financial traces are available as a resource for all levels of terrorism investigative activity. These requests are made to the CIA National Clandestine Service (NCS), which maintains classified, foreign financial transaction data. Sensitive financial traces differ from normal CIA names traces. Obtaining access to the data available from a sensitive financial trace requires a separate request.

(S//NF) Requests for sensitive financial traces must be made via EC to the appropriate TFOS unit and CTD program management unit under the TERRFIN subfile of the respective investigation. Upon receipt of the EC requesting a sensitive financial trace, TFOS will review the request and draft the appropriate cable for NCS.

17. (U//FOUO) Net Talon National Initiative

(S//REL TO USA, FVEY) Terrorists' use of the Internet has presented the FBI, the USIC, law enforcement, and U.S. allies with a serious challenge. The Internet is a principal tool for terrorist organizations in countering the physical dispersal and decentralization brought on by the American and allied response to the September 11, 2001, attacks. The perceived anonymity, security, and efficiency of online communications have attracted the attention of terrorists, their facilitators, and their sympathizers. The result has been an explosive growth of terrorists using the Internet for communications, propaganda dissemination, fundraising, recruitment, operational planning, training, and radicalization. Efforts by the FBI and its partners to investigate, exploit, and disrupt terrorist networks are being challenged by the rapid growth of terrorists' use of the Internet. In May 2008, the NTNI was approved by CTD. The NTNI is constructed to strategically focus operations targeting terrorists' use of the Internet through OCEs, UCEs, and CHSs.

> **Note:** (U//FOUO) Not all Group I UCOs will be incorporated into the NTNI. Each operation will be evaluated on an investigation-by-investigation basis, and a determination made based upon several criteria, including scope, goals, and objectives.

17.1. (U//FOUO) Net Talon Goals

(S//REL TO USA, FVEY) The goals of the NTNI are:

- (S//REL TO USA, FVEY) To detect, penetrate, disrupt, and dismantle online terrorist networks.
- (S//REL TO USA, FVEY) To know, monitor, and target an adversary's online domain.
- (S//REL TO USA, FVEY) To identify, direct, and recruit the most appropriate FBI online resources to target U.S. adversaries and their online domains.
- (S//REL TO USA, FVEY) To develop and manage online resources to maximize HUMINT penetration into online terrorist networks.
- (S//REL TO USA, FVEY) To establish and support standard operating procedures for Group I UCOs targeting terrorists' use of the Internet.
- (S//REL TO USA, FVEY) To establish standardized training for appropriate NTNI personnel.

17.2. (U//FOUO) Net Talon Objectives

17.2.1. (U) Effective Tasking of Undercover Personnel

(S//REL TO USA, FVEY) The establishment of the NTNI allows visibility into the online activities of all OCEs, UCEs, and CHSs targeting IT subjects and provides a program to ensure they are tasked according to their skill sets and workloads. The use of OCEs, UCEs, and CHSs is warranted when it is prudent and necessary to provide support and/or assistance to ongoing investigations.

17.2.2. (U) Centralized Deconfliction

(S//REL TO USA, FVEY) The NTNI establishes the centralized methods that will be used to deconflict targets, OCEs, UCEs, and CHSs within the FBI, the USIC, and international partners. For more information, refer to subsection 17.5 of this PG regarding the Net Talon Database.

17.2.3. (S//NF) Joint Operations with USIC and International Partners

(S//NF) To meet the FBI's mission of intelligence collection and to respond to investigative program priorities at national and/or international levels, it is necessary for the FBI to conduct joint operations with the USIC and international partners. The NTNI will support these joint operations and has the capability to utilize all the resources and tools available to the FBI, USIC, and international partners.

17.2.4. (U) Focused Strategic and Tactical Analytical Capability

(S//REL TO USA, FVEY) A significant component in nearly every IT investigation is acquiring enough analytical resources to analyze and disseminate the information collected. In the past, these resources were limited to the amount of personnel in a particular FO and their relevant skill sets. The NTNI creates single points of contact within the FBI that are "centers of expertise" for a particular target set or communication platform.

(S//REL TO USA, FVEY) These centers of expertise help to produce analytic products to enhance the knowledge of terrorists' use of the Internet, develop tools for identifying and dismantling online terrorist networks, and share trends in terrorists' use of the Internet. It is understood that targets may cross centers of expertise. As such, CITU is responsible for both ensuring deconfliction between the centers of expertise and for coordination of effort.

(S//REL TO USA, FVEY) The centers of expertise provide the FBI, USIC, and international partners the ability to draw upon the knowledge and resources of the centers in their investigations. NTNI analytic products and reporting are disseminated to the FBI, USIC, and international partners, as appropriate.

17.2.5. (U) Identify and Address Intelligence Gaps

(S//REL TO USA, FVEY) The NTNI addresses known intelligence gaps and identifies online terrorist networks in a centralized manner, consistent with the AGG-Dom and DIOG. The initiative's cohesive analytic capabilities allow for straightforward recognition of intelligence gaps and comparison of newly established threats. Simultaneously, a network of associated UCOs effectively addresses those intelligence gaps.

17.2.6. (U) Establishment and Sharing of Best Practices

(S//REL TO USA, FVEY) The centralizing nature of the NTNI lends itself to the improved discovery and promulgation of best practices. In the past, best practices were often limited to a single FO or shared only through informal discussions between FBIHQ, FOs, and the USIC. The NTNI captures, disseminates, and shares the tools and methods that have proven effective and useful in investigating terrorists' use of the Internet. These best practices are shared and formalized in training, guidance, and communication documents.

17.2.7. (U) Centralized Intelligence Dissemination

(S//REL TO USA, FVEY) A key component of NTNI is its ability to function as a clearinghouse for all FBI intelligence regarding terrorists' use of the Internet and the collective response to the threats posed. Previously, reporting from individual operations was sent to numerous units within CTD and CyD. The result of that system was fragmented, compartmentalized intelligence and an inability to see and communicate a comprehensive view of terrorists' use of the Internet.

(S//REL TO USA, FVEY) Under NTNI, intelligence reporting on the terrorists' use of the Internet can be centralized under CITU, which will appropriately coordinate with other units within the FBI, as well as with USIC and international partners.

(S//REL TO USA, FVEY) When an FO determines that information from any OCE, UCE, CHS, and/or Group I UCO under the NTNI affects investigative matters in another FO, the appropriate FBIHQ unit must be notified, and the information forwarded to the other FO under that office's investigative file. All communications must be properly uploaded to the FBI's permanent system of records, unless extraordinary circumstances necessitate an exception to this requirement and the exception is approved by the Deputy Director (DD).

17.2.8. (U) Centralized Resource Identification and Tracking

(S//REL TO USA, FVEY) A recurring benefit of NTNI is centralizing the management of information and resources. With the establishment of this initiative, CITU and CTUC are the central authorities over resources available to target, analyze, and exploit potential terrorist activity online. Additionally, NTNI has established tools and methods for tracking the allocation of such resources.

17.2.9. (U) Standardized UCO Administrative Tasks

(S//REL TO USA, FVEY) The NTNI standardizes the administrative tasks, as well as policy and guidelines of Group I UCOs targeting terrorists' use of the Internet. Standardized language will be created and utilized in documentation relative to CT online UCOs.

17.2.10. (U) Consistent Backstopping

(S//REL TO USA, FVEY) Central to all online UCOs is maintaining the security of covert operations. Protecting the true identity of any OCE, UCE, and/or CHS is always the primary concern in any decision related to these operations. This principle extends even to the decisions to disseminate the identities within DOJ and among JTTF partners. The NTNI standardizes the backstopping process and procedures for Group I UCOs targeting terrorists' use of the Internet. Prior to deploying online resources, all NTNI Group I UCOs must meet minimum backstopping requirements, in coordination with CITU and CTUC. See the [redacted] and the [redacted] for additional information.

17.2.11. (U//FOUO) Net Talon Organizational Structure

(S//REL TO USA, FVEY) The NTNI serves as an organizational tool to bring similar CT Group I UCOs targeting terrorists' use of the Internet under the program management of CITU. CITU exploits intelligence to track current trends of terrorists' use of the Internet, as well as reviews

reporting to uncover links between various online UCOs. CITU also conducts administrative taskings to include the tracking, collection, and compilation of OIA.

(S//REL TO USA, FVEY) A franchise operation (FOP) is a Group I UCO that falls under the NTNI. FOPs are the center of expertise for their target set or communication platform, and approve the usage of OIA authorities and coordinate with CITU for all operational matters. Suboperations (SO) fall within the scope of an existing FOP, and report directly to the FOP for operational coordination. The NTNI organizational chart is listed below in Figure 1.

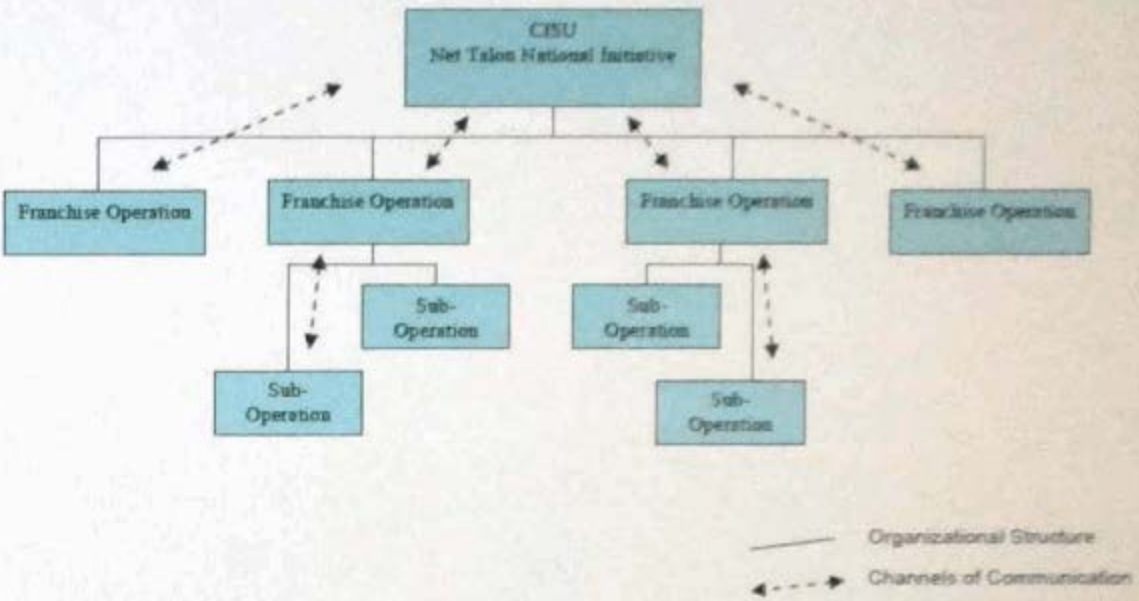


Figure 1. (U//FOUO) NTNI Organizational Chart

17.3. (U//FOUO) Net Talon Roles and Functional Responsibilities

17.3.1. (U) Counterterrorism Internet Targeting Unit

(S//REL TO USA, FVEY) CITU is responsible for the overall program management of the NTNI and the FOPs under the NTNI. CITU must:

- (S//REL TO USA, FVEY) Assign and prioritize investigations and leads for FOPs, including:
 - (S//REL TO USA, FVEY) Be the lead for the FBI's efforts within the FBI, the USIC, and with international partners to deconflict UCOs targeting terrorists' use of the Internet.
 - (S//REL TO USA, FVEY) Deconflict assignment of OCEs, UCEs, and CHSs and targeting of subjects.

- (S//REL TO USA, FVEY) Deploy, manage, and maintain the Net Talon Database for the deconfliction and program management of resources.
- (S//REL TO USA, FVEY) Conduct routine audits to ensure all profile and persona information in the Net Talon Database is current and accurate.
- (S//REL TO USA, FVEY) Review, assign, prioritize, and track requests to target CTD investigative subjects with an Internet nexus.
- (S//REL TO USA, FVEY) Periodically conduct an overall FBI strategic review to determine when new investigations targeting terrorists' use of the Internet need to be opened. Validation is an ongoing process to monitor, review, assess, and evaluate an FOP. CITU will utilize reasonable methods to validate the purpose and mission of the FOPs and ensure they are prioritized within the goals and objectives of CTD.
- (S//REL TO USA, FVEY) Receive and review intelligence disseminations for FOPs, SOs, OCEs, UCEs, and CHSs to:
 - (S//REL TO USA, FVEY) Exploit intelligence to track current trends of terrorists' use of the Internet.
 - (S//REL TO USA, FVEY) Review and analyze reporting to uncover links between various investigations, and provide this analysis to the appropriate entities.
- (U//FOUO) Coordinate with CTUC to ensure all OCEs and UCEs are properly certified, trained, and safeguarded prior to being operational on any of the NTNI's undercover operations. CITU also ensures that training is made available for contact agents who work with OCEs, UCEs, and CHSs. See the [redacted] and the [redacted] for additional information.
- (U//FOUO) Assist CTUC in the development of specialized training.
- (U//FOUO) Review and apply for OIA authority, as necessary, for FOPs. Coordinate with FOPs to ensure the language and scope for OIA authorities that benefit the entire NTNI are optimized. All OIA requests must be submitted to NSLB for approval.
- (U//FOUO) Manage, train, and provide oversight of the operational use of OIA authorities.
- (U//FOUO) Collect OIA authority usage from FOPs and provide the proper reporting to NSD's Counterterrorism Section (CTS) regarding the OIA within the stated time frame.
- (U//FOUO) Propose, manage, and allocate budget funds in support of the NTNI major investigation.
- (U//FOUO) Assist in the preparation and presentation of UCO initiation and renewal paperwork, in accordance with NSB undercover policy for all FOPs that will fall under the program management responsibility of the NTNI.

- (U//FOUO) Work with CTUC to determine whether an existing UCO or proposed FOP falls within the scope of the NTNI. In addition, CTTU will help determine if and when an SO will transition into an FOP.
- (U//FOUO) Provide the means and infrastructure for ensuring consistent intelligence collection, reporting, dissemination, and deconfliction.
- (U//FOUO) Recruit, develop, and train OCEs, UCEs, and CHSs in coordination with CTUC, the FOP, and in certain instances CHOU or the Language Services Section (LSS).
- (U//FOUO) Coordinate with FOPs on all issues concerning the LSS, as applicable to the NTNI.
- (U//FOUO) Coordinate communications and intelligence disseminations between the FBI, USIC, and international partners for all FOPs under program management of the NTNI.
- (U//FOUO) Carry out ELSUR procedures, as determined by the DIOG, the Operational Technology Division's (OTD) Data Intercept Technology Unit (DITU), and RMD's ELSUR Operations Unit.

17.3.2. (U) Counterterrorism Division Undercover Operations Unit

(U//FOUO) CTUC is responsible for the oversight and management of all UCOs that fall within the scope of the NTNI and must specifically:

- (U//FOUO) Work with CTTU to determine whether an existing UCO or proposed FOP falls within the scope of the NTNI. In addition, CTUC helps determine if and when an SO will transition into an FOP.
- (U//FOUO) Coordinate with CTTU and NSLB to submit any proposed FOP for Group I UCO review by the National Security Undercover Review Committee (UCRC), and obtain approval by the AD, CTD, according to standards established by the NSUCO PG (0307PG).
- (U//FOUO) Review all policies and procedures of the NTNI and provide guidance, as necessary, to conform to CTUC standards.
- (U//FOUO) Coordinate with CTTU to ensure OCEs and UCEs are properly certified, trained, and safeguarded prior to operational activities. CTUC works with CTTU to ensure that appropriate training courses are developed and implemented, as needed. See the [redacted] for additional information.
- (U//FOUO) Work in coordination with CTTU, FOP, and in certain instances CHOU or the LSS, to recruit, develop, and train OCEs, UCEs, and CHSs.

17.3.3. (U) Franchise Operations

(S//REL TO USA, FVEY) An FOP is a Group I UCO that has been approved by the UCRC with its own operating budget, which is managed as part of the NTNI. The FOP will be a center of expertise for its target set or communication platform, and its responsibilities include:

- (U//FOUO) Have at least one contact agent and one OCE and/or UCE.
 - (U//FOUO) No one may serve within the same FOP as both an OCE or a UCE **and** the case agent for the FOP.
- (U//FOU) Coordinate with CITU on all investigative matters.
- (U//FOUO) Coordinate with CITU, CTUC, and other necessary entities regarding the targeting strategy to be implemented by the contact agents, OCEs, UCEs, and CHSs whom the FOP directly operates and manages.
- (U//FOUO) Ensure that the predication for all investigative subjects targeted through the FOP is sufficiently articulated in the appropriate FOP documents.
- (U//FOUO) Approve the usage of OIA authorities for OCEs, UCEs, and CHSs. The FOP summarizes the usage of OIA and report to CITU, as stipulated in the operating OIA. Further, the FOP is responsible for ensuring all reporting requirements are met.
- (U//FOUO) Monitor all OCEs, UCEs, and CHSs to ensure they are operating in compliance with all applicable legal and policy requirements and direction.
- (U//FOUO) Handle requests for equipment or other resources from contact agents, OCEs, UCEs, and CHSs.
- (U//FOUO) Disseminate intelligence from OCE, UCE, and CHS reporting, in coordination with CITU.
- (U//FOUO) Recruit, develop, and train OCEs, UCEs, and CHSs, in coordination with CITU.
- (U//FOUO) Enter and update OCE, UCE, and CHS information in the Net Talon Database for deconfliction and program management purposes.
- (U//FOUO) Conduct routine audits to ensure all profile and persona information in the Net Talon Database is current and accurate.
- (U//FOUO) Write and submit Group I UCO proposals/renewals to CTUC and CITU. Draft proposals/renewals will be submitted to CTUC and CITU for review prior to obtaining local signatures.
- (U//FOUO) Disseminate reporting to CITU and the appropriate FOs. In addition to any appropriate investigative files, FOPs will ensure all OCE, UCE, and CHS communications are captioned to the assigned subfile under the NTNI investigative file, [redacted].
- (U//FOUO) Ensure that required backstopping is done for all OCEs, UCEs, and CHSs involved in an operation.

 (U//FOUO) Concerns regarding OCE or UCE personnel must be addressed with CTUC, CITU, and the contact agent.

- (U//FOUO) Ensure coordination with the case agent concerning the subject being targeted through the FOP.
- (U//FOUO) Provide trainers who will be utilized in conducting specialized training by CITU and CTUC, as requested.
- (U//FOUO) Work in coordination with CITU, CTUC, and in certain instances CHOU or LSS, to recruit, develop, and train OCEs, UCEs, and CHSs. The FOP utilizes reasonable methods to validate a CHS's identity, information, motivation, and access. Once a CHS has been recruited, the FOP is required to comply with the *Confidential Human Source Policy Guide* (0499PG) on all matters regarding a CHS.

17.3.4. (U) Suboperations (SO)

(U//FOUO) An SO must fall within the scope of an existing FOP and is developed in coordination with the FOP and CITU, with the intent of becoming a UCRC-approved FOP, where appropriate. SOs are not independent FOPs, but rather, work under the authorities and the funding of an existing FOP. Refer to subsection 17.7.5. of this PG for the process of initiating an SO. The responsibilities of an SO are to:

- (U//FOUO) Fall within the targeting set of the FOP.
- (U//FOUO) Have at least one contact agent and one OCE, UCE, or CHS.
 - (U//FOUO) It is not recommended that the primary case agent be an OCE or a UCE of the SO.
 - (U//FOUO) There must be at least one individual of the SO who is not an OCE or a UCE.
- (U//FOUO) Report directly to the FOP for investigative coordination and receive CITU assistance, as necessary.
- (U//FOUO) Coordinate with the FOP on the targeting strategy to be implemented by OCEs, UCEs, and CHSs operating under the SO.
- (U//FOUO) Ensure that the predication for all investigative subjects targeted through the SO is sufficiently articulated in the appropriate SO documents.
- (U//FOUO) Request the usage of OIA authorities for OCEs, UCEs, and CHSs from the FOP. The SO summarizes the usage of OIA authorities and report to the FOP as stipulated in the operating OIA authority.
- (U//FOUO) Monitor all OCEs, UCEs, and CHSs to ensure they are operating in compliance with all applicable legal and policy requirements and direction.
- (U//FOUO) Submit requests received from contact agents, OCEs, UCEs, and CHSs to the FOP for equipment or other resources.
- (U//FOUO) Disseminate intelligence from OCE, UCE, and CHS reporting, in coordination with the FOP and CITU. Ensure all OCE, UCE, and CHS communications

are captioned to the appropriate investigative files and assigned subfile under the NTNI investigative file [redacted]

- (U//FOUO) Initiate appropriate investigations of targets of interest that are within the scope of the SO.
- (U//FOUO) Upon the direction of the FOP, CITU, and CTUC, draft and obtain local approval for a Group I UCO to become an FOP, as part of the NTNI.
- (U//FOUO) Conduct routine audits to ensure all profile and persona information in the Net Talon Database is current and accurate.
- (U//FOUO) Work in coordination with CITU, CTUC, and in certain instances CHOU or LSS, to recruit, develop, and train OCEs, UCEs, and CHSs. The SO utilizes reasonable methods to validate a CHS's identity, information, motivation, and access. Once recruited, the SO is required to comply with the *Confidential Human Source Policy Guide* (0499PG) on all matters regarding a CHS.
- (U//FOUO) Address concerns regarding OCE or UCE personnel with CTUC, CITU, the FOP, and the contact agent.

17.3.5. (U) Contact Agents

(U//FOUO) The contact agent's primary responsibility is to manage OCEs, UCEs, and CHSs by acting as an intermediary for all communication from the NTNI and FOs whose investigations are being supported by the NTNI. Specifically, the contact agent must:

- (U//FOUO) Ensure that OCEs, UCEs, and CHSs have proper backstopping and training for the tasks they are asked to complete.
- (U//FOUO) Ensure full compliance with the required paperwork for the participation of OCEs, UCEs, and CHSs in the NTNI.
- (U//FOUO) Provide guidance to OCEs, UCEs, and CHSs for the implementation of the targeting strategy and legend building. See the [redacted] for more information.
- (U//FOUO) Monitor all OCEs, UCEs, and CHSs to ensure they are operating in compliance with all applicable legal and policy requirements and direction.
- (U//FOUO) Review OCE, UCE, and CHS reporting documents for dissemination through the NTNI FO reporting chain. Ensure that threat information is immediately disseminated in the appropriate form to the proper parties.
- (U//FOUO) Address concerns regarding OCE or UCE personnel with CTUC, CITU, and the case agent.
- (U//FOUO) Ensure FOP coordination with the case agent concerning the subject being targeted by the OCE, UCE, and/or CHS.

- (U//FOUO) Submit requests for new equipment, technical issues, or OIA authority to the responsible FOP.
- (U//FOUO) Complete the appropriate accomplishments within the accomplishments module of the FBI's central recordkeeping system for OCEs and/or UCEs.
- (U//FOUO) Complete the appropriate "CHS Report Document" [redacted] statistical accomplishment report for CHSs).
- (U//FOUO) Ensure all CHS handling and operation is in compliance with the *Confidential Human Source Policy Guide* (0499PG).
- (U//FOUO) Work with OCEs, UCEs, and CHSs to identify, assess the suitability of, and validate other individuals who may be recruited as CHSs online.
- (U//FOUO) If the OCEs, UCEs, and/or CHSs are permanently stationed and conducting operations within another FO's territory, the contact agent must have documented concurrence from all of the involved FOs.
- (U//FOUO) Keep the case agent apprised of information impacting the operations of other FOs and/or government agencies that the OCE, UCE, and/or CHS is supporting.
- (U//FOUO) Coordinate all requests for subject targeting with CITU.
- (U//FOUO) Ensure all OCE, UCE, and CHS online identities supporting CT investigations are entered into the Net Talon Database and updated, as necessary.
- (U//FOUO) Protect the identities of all OCEs, UCEs, and CHSs for whom they are responsible.

 (U//FOUO) **Note:** CHS handlers must abide by the *Confidential Human Source Policy Guide* (0499PG), which has priority over this document.
- (U//FOUO) Linguist OCEs must provide written feedback on their performance to LSS, in coordination with the case agent. Refer to subsection 17.4.4. of this PG for additional information.
- (U//FOUO) Be familiar with, and, as appropriate, use the "Checklist for Agents Handling Online CHSs" provided on the CTD Templates Page.

17.3.6. (U//FOUO) Undercover Employees

(U) A UCE's responsibilities, with regard to NTNI, are as follows:

- (U//FOUO) Successfully complete specialized training deemed appropriate by CITU and/or CTUC, in addition to the required, standard UCE training.
- (U//FOUO) Follow tasking and guidance from the contact agent who has been assigned to the FOP or SO.
- (S//REL TO USA, FVEY) Assist in identifying, assessing the suitability of, and validating potential CHSs online.

- (U//FOUO) Coordinate all requests for subject targeting with the contact agent, who will then coordinate with CITU.
- (S//REL TO USA, FVEY) Ensure all online identities supporting CT investigations are entered into the Net Talon Database and updated, as necessary.

(U//FOUO) While certified UCEs may work in an online role, they will also have the flexibility to handle face-to-face/physical world operations against the subjects of the NTNI.

17.3.7. (U//FOUO) Online Covert Employees

(U) An OCE's responsibilities, with regard to NTNI, are as follows:

- (U//FOUO) OCEs are required to successfully complete specialized training deemed appropriate by CITU and/or CTUC in addition to the standard OCE training.
- (U//FOUO) Follow tasking and guidance from the contact agent who has been assigned by the FOP or SO.
- [redacted]
- (S//REL TO USA, FVEY) Assist in identifying, assessing the suitability of, and validating potential CHSs online.
- (S//REL TO USA, FVEY) Be available to testify concerning the OCE's online covert activities if an investigation goes to trial. If the OCE is unwilling to testify, this may preclude the OCE's ability to target certain subjects.
- (U//FOUO) Coordinate all subject targeting requests with the contact agent, who will then coordinate with CITU.
- (S//REL TO USA, FVEY) Ensure all online identities supporting CT investigations are entered into the Net Talon Database when they are created and updated.

17.3.8. (U//FOUO) Confidential Human Sources

(U//FOUO) The following policies must be followed with regard to CHS participation in the NTNI, in addition to the general CHS policies outlined in the *Confidential Human Source Policy Guide* (0499PG):

- (U//FOUO) The NTNI utilizes CHSs in FOPs and SOs in order to respond to investigative priorities and FBI intelligence collection requirements.
- (U//FOUO) Intelligence collected from CHSs may be disseminated, pursuant to proper dissemination procedures, to members of the intelligence and law enforcement communities, in order to support the USG's national security and law enforcement objectives.

- (U//FOUO) A CHS will collect information on the NTNI investigative priorities, as well as assist in identifying, assessing the suitability of, and validating potential CHSs.
- (U//FOUO) Handling agents must protect the identities of all CHSs for whom they are responsible.
- (U//FOUO) A CHS may be required to sign a nondisclosure agreement to protect the sensitive nature of his or her relationship within the NTNI and to avoid jeopardizing the effectiveness of the operation.

17.3.9. (U//FOUO) Case Agents of Subjects Targeted Through NTNI

(U//FOUO) The case agent of a subject targeted through NTNI provides operational oversight of all aspects of an investigation regarding that subject, specifically:

- (U//FOUO) If the case agent of an NTNI subject needs assistance identifying the appropriate FOP, he or she may contact CITU for information regarding the capabilities of each FOP.
- (U//FOUO) To request assistance, the case agent of the subject coordinates with the case agent of the FOP and submits a formal request, as stipulated by the FOP.
- (U//FOUO) The case agent of an NTNI subject provides the FOP with information about the subject and participates in the development of an operational plan.
- (U//FOUO) The case agent of an NTNI subject is responsible for providing the FOP with feedback regarding the usefulness of the reporting generated from the investigation.
- (U//FOUO) The case agent of an NTNI subject, in coordination with the FOP, is responsible for disseminating the intelligence generated from the activities of the FOP that are pertinent to the investigation.

17.3.10. (U) Other Government Agency Partners

(S//REL TO USA, FVEY) Recent FBI efforts to investigate terrorists' use of the Internet have yielded excellent relationships with USIC partners and have resulted in the development of numerous joint operations with OGAs or international partners. Upon request, the NTNI may be utilized to support OGAs, both international and domestic. The following factors must be considered when determining whether the FBI will assist another government agency utilizing the NTNI:

1. (U//FOUO) Situations in which the FBI or the other agency serves as the primary point of contact with the OCE, UCE, and/or CHS in the investigation.
2. (U//FOUO) The degree of contact the OCE, UCE, and/or CHS maintains with the FBI and/or the OGA.
3. (U//FOUO) The priority of the target.
4. (U//FOUO) Situations in which the FBI directly tasks the OCE, UCE, and/or CHS.

5. (U//FOUO) Situations in which a particular operation primarily supports a specific FBI investigation and/or goal or objective.

(U//FOUO) The NTNI seeks to utilize other agencies' resources, when necessary, in the most efficient manner.

17.4. (U) Net Talon OCE Linguist Program

(S//REL TO USA, FVEY) The DI's LSS/Language Services Translation Center (LSTC) serves as the central coordinator of linguist support to the NTNI and related investigations by identifying linguists to serve as OCEs.

17.4.1. (U) Requesting Linguist Support

(S//REL TO USA, FVEY) When an FOP or an SO has a need for a linguist to act as an OCE in an NTNI-related investigation, the case agent must contact CITU and CTUC for an initial discussion and an evaluation of the request. Linguists will NOT be approached by the FOP or SO. CITU and CTUC will then outline the requirements for the operation in an EC to the appropriate LSTC for assistance.

(U//FOUO) LSTC canvasses FOs in order to determine the availability of linguists with the required language and subject matter skill sets to support such a request. LSTC will then provide CITU and CTUC with the name(s) of the identified linguist(s). Any changes or modifications to the initial request for support must be cleared through the LSTC to ensure that top FBI priorities remain covered.

17.4.2. (U) Training and Safeguard Assessment

(U//FOUO) Linguist OCEs are required to meet all training and safeguard assessment stipulations set forth in subsection 17.6.9. of this PG.

17.4.3. (U) Quality Control

(U//FOUO) All linguists working for the FBI are subject to LSS's quality-control process (refer to [redacted] and are required to have samples of their work reviewed, in accordance with established policies. Quality control will provide an additional backstop to ensure that complete and correct information is being conveyed to the Net Talon case agents.

(U//FOUO) Given the sensitive nature of the UCO materials, CITU will coordinate with the Quality Control and Standards Unit in LSS to ensure that appropriate work samples are submitted by the contact agent, in coordination with the case agent, for quality control review in a predetermined time frame.

17.4.4. (U) Required Feedback on Linguist Performance

(U//FOUO) In order to effectively give feedback to linguist OCEs for progress reviews, performance appraisal reports, and annual work reviews, the contact agent, in coordination with the case agent, may be asked to provide written performance feedback.

17.4.5. (U//FOUO) Removing Linguists from the NTNI

(U//FOUO) Linguist OCEs have the right to withdraw from the UCO program at any time for personal or professional reasons.

(U//FOUO) If at any point, CTIU and/or CTUC determine that a linguist is not suitable to remain in the OCE program, CTIU and/or CTUC will inform LSTC in writing. If CTIU, CTUC, or LSTC removes a linguist from the OCE program, barring other performance concerns, no jeopardy will be attached to the linguist in question that would preclude the linguist from taking other NTNI assignments.

17.5. (U//FOUO) Net Talon Database

(S//REL TO USA, FVEY) To address the need for a centralized method of online deconfliction within the FBI, CTIU has taken the lead and, in collaboration with the Special Technologies and Applications Office (STAO), developed the Net Talon Database (refer to [redacted]). All OCE, UCE, CHS, and available USIC and foreign partner online information must be entered into the database for purposes of deconfliction for online personas and effective program management of online HUMINT. **The true name of the OCE, UCE, or CHS is not stored in the system, only the symbol number and point of contact.** The database will be available FBI-wide to determine if an unknown online moniker or facility is a United States and/or foreign government equity.

(U//FOUO) The specific purposes for the Net Talon Database include:

- (U//FOUO) Providing a real-time deconfliction mechanism over the FBI Intranet to all FBI users.
- (S//REL TO USA, FVEY) Creating a comprehensive, searchable directory of all online identities targeting IT investigations, including e-mail addresses, screen names, monikers, and pseudonyms.
- (S//REL TO USA, FVEY) Creating a centralized repository of available online resources that will capture language abilities, cultural and religious expertise, and other skill sets that can be used in identifying the appropriate resources to deploy online.

17.5.1. (U) Information Stored in Net Talon Database

(S//REL TO USA, FVEY) The true names of OCEs, UCEs, and CHSs may not be entered into the database. This includes any approximated information such as online personas or facilities that would reveal the true identities of these individuals.

(S//REL TO USA, FVEY) Characteristics of the true identity of an OCE, a UCE, or a CHS must be entered into the database as the **profile**. This information may include the following:

- (U//FOUO) Symbol number
- (U//FOUO) Type (OCE, UCE, or CHS)
- (U//FOUO) Originating FO
- (U//FOUO) Contact agent (name, division, and contact phone)

- (U//FOUO) Age range
- (U//FOUO) Gender
- (U//FOUO) Skill sets (e.g., languages, cultural knowledge, regional knowledge, education, hobbies, religion)
- (U//FOUO) Ethnic background
- (U//FOUO) Religious background
- (U//FOUO) Experience (e.g., past employment, education, travel)
- (U//FOUO) Investigations (file numbers of current and previous investigations on which the employee has worked)

(S//REL TO USA, FVEY) Information relating to the online identities associated with the OCE, UCE, or CHS must be entered into the database as **personas**. This information is linked to the profile page and will include the following:

- (U//FOUO) Persona name
- (U//FOUO) Legend (see [redacted]
- (S//REL TO USA, FVEY) Facilities (type [e.g., e-mail, instant message (IM), blog], moniker, screen name, legend, creation date, deactivation date)
- (U//FOUO) Creation date
- (U//FOUO) Active/inactive
- (U//FOUO) Deactivation date

(S//REL TO USA, FVEY) When available, USIC and foreign partner online information is entered into the database.

(U//FOUO) CITU will have the ability to add additional selectors to allow a more accurate representation of the skills and characteristics of the profiles and personas.

17.5.2. (U) Levels of Access

(U//FOUO) The Net Talon Database allows FO investigators two levels of access, dependent upon their assignments, with a third level of access reserved to program management personnel.

- Level 1 - (S//REL TO USA, FVEY) Access is available to all users with access to the FBI Intranet, and does not necessitate a user name and password. It allows for simple, limited queries involving source identities, including online screen names, monikers, and e-mail addresses. Positive results will be noted, but not detailed, and only a point of contact for the "conflicted" source will be provided.
- Level 2 - (U//FOUO) Access allows case agents and selected investigative personnel the same capabilities as Level 1 access, with the added capabilities to edit and add data. Users are only able to access records that they have created or to which they have been delegated access.

- Level 3 - (U//FOUO) Access is reserved for specified CITU personnel assigned the responsibility of maintaining the integrity and accuracy of the database. This access allows CITU the ability to immediately search, identify, and allocate resources that are most suitable for a particular FOP.

17.5.3. (U) Entering and Updating Information

(S//REL TO USA, FVEY) All OCEs, UCEs, and CHSs supporting IT investigations are required to have profiles with their personal characteristics created in the database. It is required that every online identity associated with an OCE, a UCE, or a CHS supporting IT investigations be entered into the database when the profile and/or the identity is created.

(S//REL TO USA, FVEY) It is the responsibility of CITU and the FOP to conduct routine audits to ensure all profile and persona information is current and accurate. The ultimate responsibility for ensuring that all profile and persona information is entered and updated in the database in a timely fashion is the responsibility of the case agent.

17.5.4. (U) Requesting an Account

(S//REL TO USA, FVEY) Only users who are required to enter information into the database will need an account. To request an account, send an e-mail to [redacted] with the following information:

- (U//FOUO) Name (first, middle initial, last)
- (U//FOUO) Trilogy login
- (U//FOUO) Employee type (agent, analyst, contractor, linguist, other)
- (U//FOUO) Supervisor's name
- (U//FOUO) FO
- (U//FOUO) Phone number
- (U//FOUO) Justification for needing an account

17.6. (U//FOUO) Other Net Talon Policies

17.6.1. (U) Targeting Priorities

(U//FOUO) The subjects of the NTNI will be prioritized according to the CTD mission (refer to subsection 2.3. of this PG) and other relevant strategy and objective guidance (refer to [redacted] and [redacted]

17.6.2. (U) Subjects/Targets of the NTNI

(S//REL TO USA, FVEY) The target of an NTNI operation must be the predicated subject of an ongoing IT PI or full investigation.

(S//REL TO USA, FVEY) In order for an OCE, a UCE, or a CHS to visit facilities such as a Web site message forum, blog, or other Internet facility, that activity must be relevant to a predicated investigation, for the purpose of obtaining substantive intelligence/evidence on a

subject of an investigation, or for building bona fides. During an authorized visit, an OCE, a UCE, or a CHS may identify other subjects through passive monitoring or active communication on these Web sites.

(S//REL TO USA, FVEY) Communications with a nonpredicated individual cannot be designed to collect intelligence on that nonpredicated person. If, through building bona fides, or collecting intelligence on a predicated subject, an OCE, a UCE, or a CHS identifies an individual who makes statements that predicate that person as an IT subject, then a PI or a full investigation must be opened on that individual to continue undercover contacts designed to collect intelligence or evidence on that individual.

(S//REL TO USA, FVEY) OCE, UCE, and CHS reporting must state the reason for the communication (e.g., for building bona fides or to communicate with a predicated subject or an associate of a predicated subject of an investigation) and how the communication is relevant to the investigation. For example, if the reason for the communication is to build bona fides, the reporting will include language similar to the following: "Online activity conducted for the purpose of building the [OCE's, UCE's, or CHS's] bona fides." In this example, this statement must include how the communication built bona fides and may not be a mere conclusory statement.

(S//REL TO USA, FVEY) If the reason for the communication is in further support of the captioned investigation, the reporting will include language similar to the following: "Online activity conducted with the purpose to further support the captioned investigation(s)."

(S//REL TO USA, FVEY) If any individual(s) targeted online is confirmed to be located outside the United States, notification will be provided to the appropriate Legat and the CIA. This notification will be coordinated through CITU.

(S//REL TO USA, FVEY) Under certain circumstances, OCEs, UCEs, and CHSs may be in contact with individuals who are not the subjects of predicated investigations (such as for building bona fides). In accordance with the DIOG (see the subsection on authorized investigative methods in assessments and predicated investigations: interviewing and requesting information from members of the public and private entities), in order for an OCE or a UCE to engage an individual for the purpose of acquiring substantive intelligence/information about that individual and that individual's activities, the FO must first open either a PI or a full investigation on that individual. This requirement does not apply to CHSs. In accordance with the DIOG section on the use and recruitment of human sources, CHSs may initiate online contacts with subjects of assessments for the purpose of acquiring intelligence about those subjects and their activities. The specific authorities of OCEs, UCEs, and CHSs are outlined as follows:

(U) OCE and UCE Authorities

- (U//FOUO) When the purpose of an OCE or UCE initiating communication with an individual is to acquire substantive intelligence about that individual and that individual's activities, the OCE or UCE is engaging in "undercover activity," and the FO must first open a predicated investigation before the OCE or UCE may engage in such contacts.

- (U//FOUO) Once a predicated investigation is opened on a subject, an OCE or a UCE may engage in unlimited communication with associates of that predicated subject for the purpose of gaining additional intelligence or evidence on the predicated subject.
- (U//FOUO) However, if the OCE or UCE subsequently develops sufficient derogatory information regarding the associate, and the purpose of the communication changes to gathering intelligence or evidence on the associate, that associate must be predicated as the subject of an appropriate investigation prior to the OCE or UCE continuing communications.
- (U//FOUO) For the purpose of establishing bona fides and credibility, OCEs and UCEs may make postings and communicate with individuals who are neither the subjects nor the associates of subjects of assessments or predicated investigations. There is no limitation with respect to the amount of communication an OCE or a UCE may initiate in this regard.
- (S//REL TO USA, FVEY) If postings are made to establish bona fides on a message forum, and the posting receives responses from other forum users through either another posting or a direct online contact, the OCE or UCE may communicate with that user to continue building bona fides. Once predication is established with the user contacting the OCE or UCE, a PI or a full investigation must be opened before the OCE or UCE may continue communicating with that individual.
- (S//REL TO USA, FVEY) In order for an OCE or a UCE to target a Web site user whose communications indicate the user is involved in international terrorism, an appropriate predicated investigation must be initiated. See the table below regarding authorized undercover contact for UCEs and OCEs.

		Nature of Target		
		Target is not a subject of a PI or a full investigation (e.g., witness, third party).	Target is the subject of an assessment.	Target is the subject of a PI or a full investigation.
Nature of Contact	Contact to obtain intelligence about the target.	No	No	Yes
	Contact to maintain cover and credibility only, not to obtain intelligence.	Yes	Yes	Yes
	Contact to obtain intelligence relevant to the subject of a PI or a full investigation.	Yes	Yes	Yes

Table 4. (S//REL TO USA, FVEY) When Online Undercover Contact is Authorized for an OCE or a UCE

(U) CHS Authorities

- (U//FOUO) The term "undercover activities" does not apply to the activities of CHSs. The subsection of the DIOG on authorized investigative methods in assessments and predicated investigations to use and recruit human sources permits the tasking of CHSs in the course of authorized assessments. Therefore, because CHSs are not under the same restriction as FBI employees with respect to the requirement that a predicated investigation be initiated prior to targeting an individual, a CHS, unlike an OCE or a UCE, may be tasked in an assessment to acquire substantive intelligence about an individual and the individual's activities. However, before an FO may target an individual and task a CHS to acquire intelligence concerning that individual, an assessment must be initiated for an authorized purpose per the DIOG (see the section on authorized purposes).
- (U//FOUO) Once an assessment is opened on an individual, a CHS may engage in unlimited communications with associates of that subject for the purpose of acquiring additional intelligence or evidence on the subject, unless prohibited or restricted by law, regulation, or policy.
- (U//FOUO) However, if the CHS subsequently develops information regarding the associate that permits at least an assessment to be opened on the associate, and the purpose of the communications is to gather intelligence or evidence on the associate, the associate must become (at least) the subject of an assessment, prior to the CHS continuing communications.

- (U//FOUO) For the purpose of establishing bona fides and credibility, CHSs may make postings and communicate with individuals who are neither the subjects nor the associates of subjects of assessments or predicated investigations. There is no limitation with respect to the amount of communication a CHS may initiate in this regard.
- (S//REL TO USA, FVEY) If a posting is made on a message board to establish bona fides, and the posting receives responses from other forum users through either another posting or a direct online contact, the CHS may communicate with that user to continue building bona fides. If an authorized purpose for an assessment develops, an assessment must be initiated before the CHS continues to have contact with that individual.
- (S//REL TO USA, FVEY) In order for a CHS to target a Web site user whose communications indicate the user is involved in international terrorism, an authorized assessment (at least) must be initiated prior to the CHS initiating communications with that user.

		Nature of Target		
		Target is not the subject of an assessment, a PI or a full investigation (e.g., witness, third party).	Target is the subject of an assessment.	Target is the subject of a PI or a full investigation.
Nature of Contact	Contact to obtain intelligence about the target.	No	Yes	Yes
	Contact to maintain cover and credibility only, not to obtain intelligence.	Yes	Yes	Yes
	Contact to obtain intelligence relevant to the subject of an assessment, a PI or a full investigation.	Yes	Yes	Yes

Table 5. (S//REL TO USA, FVEY) When Online Undercover Contact is Authorized for a CHS

17.6.3. (U//FOUO) Online Communication

(S//REL TO USA, FVEY) An OCE may engage in oral communications, including telephone or Voice over Internet Protocol (VoIP), with the approval of the SSA overseeing the FOP to which the OCE is assigned. [redacted]

[redacted]

17.6.4. (U) Otherwise Illegal Activity

(U//FOUO) In coordination with NSD's CTS and the NSLB, CITU maintains annual blanket OIA authorizations for all FOPs under the NTNI. New FOPs are not covered by this OIA until officially notified by CITU. CITU is responsible for annual renewals of these blanket OIA authorizations. All OIA must cease at the end of the authorized period unless there is written confirmation that the OIA has been extended. The following guidelines will be followed by the NTNI in regard to OIA.

(S//REL TO USA, FVEY) As required by Section V.C. of the AGG-Dom, Section V of *The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources*, the DIOG, the *Confidential Human Source Policy Guide* (0499PG), and this PG, FBIHQ will request appropriate AD and DOJ authorization for participation in OIA that cannot be authorized by the SAC for all FOs involved in the NTNI (refer to subsection 12.7.). UCOs that transition from strictly online to face-to-face may require OIA authority separate from the blanket NTNI OIA to protect the sensitive method of targeting extremists online.

(U) Application Process

(U//FOUO) OIA authority applications must be coordinated with CITU and NSLB, who will work with NSD's CTS to obtain OIA authority.

- (U//FOUO) As each FOP is approved, the case agent must concurrently apply for the OIA authorities under the NTNI. The FOP will only need to separately apply for those authorities that are not included in the blanket OIA.
- (U//FOUO) OIA authority applications that will benefit the entire NTNI must be coordinated with CITU and NSLB.
- (U//FOUO) Requests for emergency OIA approval must be handled in accordance with the DIOG for FBI employees and in accordance with the *Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources* (AGG-CHS) for CHSs.
- (U//FOUO) At the end of the period for which the OIA was approved, the case agent must cease activity until written confirmation is provided by CITU that OIA has been renewed. Without written confirmation that OIA has been authorized for an additional period, on the day that OIA authorization ends, the case agent must send written confirmation to CITU that all activities for which OIA is required have ceased.

(U) Reporting Requirements

(U//FOUO) Below are the reporting requirements for the use of OIA in the NTNI:

- (U//FOUO) Before an FOP utilizes an OIA authority, the case agent must notify CITU. No further action will be taken until CITU provides concurrence. This allows CITU to

ensure that all necessary authorities are in place prior to engaging in OIA. If an OIA memo authorizes multiple activities, the FOP must consult with CITU prior to the first instance of each activity. This notification and confirmation may be done via e-mail.

- (U//FOUO) Contact agents must document all usage of OIA to the FOP's legal subfile, as specified in the procedures section of this document. If the FOP is using an activity authorized by the OIA for the first time, the contact agent must reference and document the FOP's prior coordination with CITU.
- (U//FOUO) The case agent must periodically provide CITU with a report summarizing the OIA authorities utilized, including a brief description of the usage and the EC serial number. As DOJ requires a 90-day report on FBI OIA activities, FOP reporting is required after an initial period of 75 days.
- (U//FOUO) Every 90 days, CITU must write a report summarizing the NTNI OIA authorities utilized.
- (U//FOUO) If an FOP is authorized to engage in OIA outside of the NTNI OIA, the FOP must compile a report summarizing the use of that authority, to be provided directly to CITU every 90 days.
- (U//FOUO) CITU forwards OIA reports to NSD's CTS for review, as necessary.

(U) Usage of OIA Authorities by Undercover Personnel

(U//FOUO) Below are the limitations on the use of OIA by OCE, UCE, or CHS personnel:

- (U//FOUO) OCEs, UCEs, and CHSs of the NTNI may utilize the NTNI's OIA authorities with proper documentation of their status as working within the auspices of the NTNI.
- (U//FOUO) All participation in OIA must be in accordance with the CHS PG and the AGG-CHS.

17.6.5. (U) Classification Guidelines

(U//FOUO) All documentation generated by personnel from the NTNI must adhere to the NSICG. This includes, but is not limited to:

- (S//REL TO USA, FVEY) The protection of the sensitive method of targeting an extremist Web site or online network (refer to subsection 9.8.).
- (U//FOUO) EC documentation of all activity conducted by OCEs, UCEs, and CHSs under the authorities of the UCO, including analysis and comments on the information collected.
- (U//FOUO) FD-1023, "CHS Reporting Document" [restricted access] documentation from information provided by a CHS.
- (U//FOUO) Verbatim translations of any text.
- (U//FOUO) ECs pertaining to subject targeting and targeting strategies.

17.6.6. (U) Prosecution Guidance

(U//FOUO) All investigations that may lead to prosecution must be coordinated with CITU, NSLB, NSD's CTS, and the investigating FO's USAO.

17.6.7. (U) Attorney General Exemptions

(U//FOUO) As necessary, all FOPs are required to individually obtain the deposit of funds AG exemption through CITU and CTUC. Additional AG exemption applications must be coordinated with CITU, CTUC, NSLB, and NSD's CTS. Refer to the *Confidential Funding Policy Guide* (0248PG).

17.6.8. (U) Training

(U//FOUO) All OCEs and UCEs for an FOP are required to meet with the FO undercover program ASAC every six months. All OCEs and UCEs are required to pass the safeguard assessment and the appropriate OCE or UCE certification course before becoming operational.

(U//FOUO) In exceptional circumstances, a noncertified OCE may be used operationally as part of the NTNI, in accordance with the requirements outlined in the [redacted]

(U//FOUO) Select NTNI personnel, including each NTNI FOP case agent, are required to attend annual NTNI training sponsored and hosted by CITU. As necessary, FOPs will be required to provide personnel for training courses sponsored by CITU and CTUC.

(U//FOUO) It is recommended that each FOP schedule a training conference for its personnel approximately six months after the annual NTNI training. At this time, OCEs and UCEs of the FOP must bring all of their UC hardware to the conference for inventory purposes. Attendance at these training conferences must be documented via EC by the FOP.

(S//REL TO USA, FVEY) Typically, CHSs will not be allowed to attend the aforementioned training courses and conferences for operational security reasons. As additional training becomes available, contact agents may be asked to attend these training courses and conferences and brief CHSs on the best practices for online targeting. For CHSs beginning their participation in NTNI operations, their online activities may be corroborated by checking the information they provide via OCE or reliable CHS verification and/or through open source and FBI database checks.

17.6.9. (U) Safeguard Assessments

(U//FOUO) A current safeguard assessment is required for all OCEs and UCEs prior to becoming operational, in accordance with the NSUCO PG. OCEs, while operational, are also required to complete an annual safeguard assessment. UCEs, while operational, will be required to complete a semiannual safeguard assessment.

17.6.10. (U) Consensual Monitoring and ELSUR Collection

(U//FOUO) For basic rules on consensual monitoring, refer to Section 18 of the DIOG. Below is additional guidance specific to the Net Talon Program.

(U//FOUO) UCEs or OCEs must complete the consent forms according to the instructions listed below. CHSs must complete the consent forms according to the instructions listed below, unless contradictory instruction is given by the CHSPG, in which case, the CHSPG must be followed.

- (U//FOUO) The true name of the OCE or UCE must not be used on the FD-472 form. Instead, the online alias or symbol number is used.
- (U//FOUO) The contact agent also writes the UCE's, OCE's, or CHS's symbol number on each form for identification purposes.
- (U//FOUO) In the address field, the FO location where the individual resides is to be used.
- (S//REL TO USA, FVEY) Until such time that the FD-472 form contains language pertaining to electronic consensual monitoring, the contact agent handwrites language on the forms to the effect of, "The individual gives consent for electronic consensual monitoring of his or her activities to include e-mail, instant messaging, Web site/forum posting, private messaging, and VoIP."

(S//REL TO USA, FVEY) For all OCE, UCE, and CHS collection, Image Capture software deemed appropriate by CITU must be used to collect all screen shots, e-mails, private messaging, and Web posting activities. Additional software is used to collect instant messaging activities. FOPs may contact CITU for guidance concerning the appropriate software.

(S//REL TO USA, FVEY) DIOG Section 18 states that all recordings pursuant to consent must be stored in ELSUR. Therefore, all one-to-one communications with a target, including communicating in e-mails, chat rooms, instant messaging, private messaging, and VoIP made by OCEs, UCEs, and CHSs, must be submitted to ELSUR via the [redacted]. All current ELSUR policies contained in the DIOG and other policies must be followed.

17.7. (U) Procedures and Processes

17.7.1. (U) Working with Other Government Agencies

(U//FOUO) CITU will coordinate all joint operations with OGAs and international partners and will give final approval for the use of contractors in an operational setting. CITU must be notified whenever information needs to be passed to OGAs, international partners, or contractors.

17.7.2. (U) Investigative File Structure

(U//FOUO) As appropriate, FOPs will use standardized subfile nomenclature set forth by the NTNI, which will be in accordance with the standards outlined in the DIOG. Each FOP will have an FO 415 file in parallel to the NTNI investigative file number. The FOP will have a subfile for every OCE and UCE under its auspices in its parallel investigative file (e.g., [redacted]).

(U//FOUO) The list of approved subfiles includes, but is not limited to:

- 1A - 1A section exhibits.
- ACCOUNT-1A - case agent copies of statements and checks.
- ACCOUNTING - case agent tracking of UCO expenditures.
- ADMIN - administrative items.

- BR - financial analyst tracking of UCO expenditures.
- BR-1A - financial analyst original statements and copies of checks.
- CE - investigation expenditures.
- DISSEMINAT - information disseminated outside the FO.
- ELA - ELSUR administrative.
- ELA1 - ELSUR original logs.
- ELA1A - ELSUR copies and logs.
- ELA1B - ELSUR transcripts.
- ELA3 - consensual monitoring records.
- INTELPROD - investigative intelligence products.
- LEGAL - OIA authorities, AG exemptions, policy, public service announcements (PSA).
- PEN - pen register report.
- RPT - CHS reporting.
- STATS - statistical accomplishments.

17.7.3. (U//FOUO) Transition to Face-to-Face Activities

[redacted]

17.7.4. (U) Initiating New Franchise Operations

(U//FOUO) The FO will work with CITU, CTUC, and NSLB to draft and submit a Group I UCO proposal for UCRC review, using standardized NTNI language. In exceptional circumstances and while awaiting UCO approval, an FO may operate as an SO of an existing FOP, with CITU and CTUC approval.

(U//FOUO) In certain instances, an FO may not have the resources to become an FOP. In those investigations, an FO may request to be added as an SO under the pertinent FOP (refer to subsection 17.7.5).

17.7.5. (U) Initiating an SO

(U//FOUO) FOs planning to initiate an SO must coordinate with CITU, CTUC, and the pertinent FOP. The requesting FO must have the approval of the management within the office's CT and, as appropriate, cyber program, to work under the auspices of the FOP. This approval must be

documented in an EC format. The level of approval required may be determined by the executive management within the requesting FO.

(U//FOUO) The EC requests concurrence from the pertinent FOP to run as an SO under its operation. If the FOP concurs with the request, the case agent requests, via EC, that CITU and CTUC coordinate with NSLB to obtain CTD approval for the inclusion of the new SO. CITU or CTUC documents CTD approval in EC format and notifies the FO and FOP. The FO may not begin operations until official notification from CITU or CTUC is received.

17.7.6. (U) Intelligence Dissemination

(U//FOUO) In order to disseminate intelligence to a foreign government partner, the contact agent will draft an EC derived from OCE, UCE, or CHS reporting and coordinate with the case agent of the related investigation. The FOP will review the EC and coordinate with CITU. CITU will obtain designated intelligence disclosure official (DIDO) approval and coordinate with the Legat and the CIA, as specified by applicable MOUs, to disseminate the intelligence.

(U//FOUO) The preceding requirement does not prevent the dissemination of raw intelligence information or finished intelligence products with appropriate recipients, in accordance with the DIOG and established Directorate of Intelligence (DI) policies. All information sharing must be appropriately documented on an FD-999, in accordance with the DIOG.

17.7.7. (U) Investigative Work Flow

(U//FOUO) Targeting requests or leads from members of the NTNI are sent to the CITU for review. CITU assigns the lead to the appropriate FOP or SO. The FOP or SO must ensure that a proper PI or full investigation is open, and the FOP sends the requesting FO an EC documenting its acceptance or rejection of the targeting request.

(U//FOUO) For a lead that has been rejected, the aforementioned EC documents the reason(s) for rejection. For a lead that has been accepted, the FOP assigns this lead to the contact agent for an appropriate OCE, UCE, or CHS.

- (U//FOUO) The contact agent coordinates targeting and intelligence dissemination with the requesting FO, documents acceptance of the lead, and provides the operational targeting plan in an EC format.
- (U//FOUO) The contact agent provides the requesting FO with status updates of the operational targeting on a periodic basis. This is documented in EC format to the operational investigative file and appropriate OCE, UCE, or CHS subfile.

(U//FOUO) Intelligence, which includes, but is not limited to, tearlines, intelligence information reports (IIR), and cables, is forwarded to CITU for informational purposes. All communications, including leads, are posted to the NTNI investigative file, [redacted]. All OCE, UCE, and CHS communications are posted to the FOP's/SO's assigned subfile under the NTNI investigative file, [redacted].

17.7.8. (U) Performance Measures

17.7.8.1. (U) Statistical Accomplishments

(U//FOUO) The contact agent is required to review all OCE, UCE, or CHS documentation and determine if and when investigative accomplishments can be claimed. The contact agent will claim statistics for the OCE, UCE, CHS, and for himself or herself. The accomplishments are posted to the FOP's STATS subfile, the substantive investigation's subfile, and the NTNI investigative file number, STATS subfile.

(U) Other Statistical Accomplishments

(U//FOUO) Under the NTNI, other measures will be established to gauge the performance of OCEs and UCEs. These will include measures similar to the current [redacted] [restricted access] form's statistical accomplishments used for CHSs.

(S//REL TO USA, FVEY) Other specific online parameters are also introduced, including the duration online, the number of postings made, the extremist online venue identified (e.g., blog or Web site), and online personas created.

17.7.9. (U) Franchise Operation Accounting and Budget

(U//FOUO) Each FOP under NTNI assigns an FBI employee to act as the investigation accountant and/or financial analyst. That person is responsible for ensuring the FOP is compliant with the guidance set forth in the *Confidential Funding Policy Guide* (0248 PG).